12-1-2024

Jamming precoding in AF relay-aided PLC systems with multiple eavessdroppers

Zhengmin Kong

Jiaxing Cui

Li Ding

Tao Huang

Shihao Yan
Edith Cowan University

10.1038/s41598-024-58735-y

Kong, Z., Cui, J., Ding, L., Huang, T., & Yan, S. (2024). Jamming precoding in AF relay-aided PLC systems with multiple eavessdroppers. Scientific Reports, 14, article 8335. https://doi.org/10.1038/s41598-024-58735-y scientific reports

Check for updates

OPEN

Jamming precoding in AF relay-aided PLC systems with multiple eavessdroppers

Zhengmin Kong[1,4], Jiaxing Cui[1,4], Li Ding[1]✉, Tao Huang[2,4] & Shihao Yan[3,4]

Enhancing information security has become increasingly significant in the digital age. This paper investigates the concept of physical layer security (PLS) within a relay-aided power line communication (PLC) system operating over a multiple-input multiple-output (MIMO) channel based on MK model. Specifically, we examine the transmission of confidential signals between a source and a distant destination while accounting for the presence of multiple eavesdroppers, both colluding and non-colluding. We propose a two-phase jamming scheme that leverages a full-duplex (FD) amplify-and-forward (AF) relay to address this challenge. Our primary objective is to maximize the secrecy rate, which necessitates the optimization of the jamming precoding and transmitting precoding matrices at both the source and the relay while adhering to transmit power constraints. We present a formulation of this problem and demonstrate that it can be efficiently solved using an effective block coordinate descent (BCD) algorithm. Simulation results are conducted to validate the convergence and performance of the proposed algorithm. These findings confirm the effectiveness of our approach. Furthermore, the numerical analysis reveals that our proposed algorithm surpasses traditional schemes that lack jamming to achieve higher secrecy rates. As a result, the proposed algorithm offers the benefit of guaranteeing secure communications in a realistic channel model, even in scenarios involving colluding eavesdroppers.

The power line channel has gained significant attention in the realm of communication networks due to its utilization of existing power line infrastructure, thus avoiding the need for additional infrastructure deployment[1]. Power line communication (PLC) has established itself as a mature technology, finding applications in various domains such as indoor, outdoor, and in-vehicle communication systems[2,3]. Meanwhile, PLC system in the home automation[4], smart grid[5–7], smart city[8] and remote sensing[9] and other fields, PLC is a strong competitor of wireless communication system. In addition, the application of PLC is not limited to the above fields, in the vehicle[10,11], aviation equipment[12], ship[13,14] and train[15] communication environment, PLC has the value of application. However, the transmission of high-frequency signals over power lines, which were not originally designed for communication purposes, poses challenges in terms of considerable attenuation over long distances. In addition to attenuation, other detrimental factors such as multipath effects resulting from impedance mismatching, distortion caused by impulsive noise[16–18], and coupling loss (when PLC is connected to the electric power grid) further degrade the quality of data transmission in power line system[19].

In addition to the aforementioned challenges faced by power line communication (PLC), the strict limitations on transmit power spectral density imposed by electromagnetic compatibility regulations further hinder its coverage capabilities. These limitations overlook the negative factors affecting PLC, thereby constraining its potential for reliable and high-capacity communication over long distances[20]. As a result, achieving robust and efficient PLC under unpredictable channel conditions becomes even more challenging. To overcome these limitations and enhance the reliability and reach of PLC networks, researchers have explored the application of relay-aided communication[21]. By leveraging relay nodes, which serve as intermediaries between the source and destination, relay-aided PLC offers promising opportunities for long-distance transmission in the high-frequency band[22].

Previous research efforts have made significant strides in the development of long-distance transmission techniques for power line communication (PLC) systems employing relay nodes[23–26]. However, it is important to note that the majority of these studies primarily concentrate on the decode-and-forward (DF) relaying protocol[25,26], with only a limited number exploring amplify-and-forward (AF) relay-aided PLC systems[24]. In

[1]School of Electrical Engineering and Automation, Wuhan University, Wuhan 430072, China. [2]College of Science and Engineering, James Cook University, Smithfield, QLD 4878, Australia. [3]School of Science, Edith Cowan University, Joondalup, WA 6027, Australia. [4]These authors contributed equally: Zhengmin Kong, Jiaxing Cui, Tao Huang and Shihao Yan. ✉email: liding@whu.edu.cn

comparison to DF relaying, AF approaches utilize simpler relay nodes that do not necessitate additional time for decoding, quantization, or digital signal processing. Through the straightforward process of amplifying and forwarding the received signals, AF relays can reduce the overall end-to-end transmission delay. Consequently, the performance of PLC systems based on AF relaying schemes has become an intriguing area of investigation, warranting further exploration.

The establishment of a reliable power line communication system necessitates the improvement of coverage and the guarantee of data rates, both of which are challenging due to power and bandwidth limitations[27]. In addition to the introduction of relay nodes, one practical approach to enhance data rates within a given channel quality is to improve spectral efficiency. In this regard, in-band full-duplex (IBFD) technology has showed up as a viable solution, originally explored in the realm of wireless communication[28–31]. IBFD enables simultaneous transmission and reception of signals within the same frequency band[32]. Furthermore, the application of IBFD can enhance the overall relaying capacity of a multi-hop network by enabling full-duplex relaying. This approach mitigates the repeating delays associated with each relay node, effectively doubling the data throughput[33]. IBFD has recently garnered significant attention in the context of PLC[34]. As a result, the development of IBFD technology holds great promise in enhancing the performance of long-distance PLC systems[35].

Another significant issue in communication is to enhance security against potential negative factors[36,37]. The cheap and ubiquitous power line system is not perfect. How to enhance the security of the communication system based on power line is a serious problem with the electromagnetic radiation in the power line and the existence of malicious wired users[38,39]. Despite the incorporation of relays and in-band full duplex (IBFD) communication, long-distance power line communication (PLC) systems are inherently more vulnerable to security risks compared to conventional wireless communication. These vulnerabilities arise from factors such as impedance mismatch and non-Gaussian noise, which are characteristic of power line channels. Furthermore, in a relay-aided PLC system, the presence of malicious users who can potentially eavesdrop on messages transmitted between the source and relay nodes poses significant security threats. The security of such systems is further compromised by imperfect channel state information (CSI), which can deteriorate the overall security posture. It is important to note that power line channels and wireless channels share similarities, including frequency selectivity, frequency-dependent attenuation, and an open nature that allows any wireless or PLC device to intercept the exchanged messages. Consequently, both types of communication channels are susceptible to exploitation by malicious users[40,41]. In light of these shared vulnerabilities, it becomes possible and necessary to leverage well-investigated wireless communication technologies and security mechanisms in the context of PLC. Existing research has already demonstrated the feasibility and importance of applying established wireless communication technologies to enhance the security of PLC systems[24,42].

The security of power line communication (PLC) can be achieved through two primary approaches: cryptographic protocols and physical layer security (PLS). While cryptographic protocols are effective in securing data transmission, PLS leverages the quality of the channel to protect against eavesdropping attacks. Compared to cryptography-based methods, PLS techniques have lower complexity and have attracted recent research interests[43]. The concept of PLS was initially introduced in the 1970s[44–46] and has since undergone extensive research. Initially, studies focused on the degraded wiretap channel[44], followed by investigations into the non-degraded wiretap channel[45,46]. More recently, research has delved into the analysis of fading wiretap channels[47,48] and multiple-input–multiple-output (MIMO) wiretap channels[49–51]. PLS has also found applications in other communication scenarios, such as fiber optical networks[52]. In the context of PLC, research efforts have explored the application of PLS in different system configurations. Studies initially concentrated on PLS for single-input, single-output (SISO) PLC systems[51], followed by investigations into PLS techniques for MIMO-based PLC systems[53].

At present, there are some related fields of research as showed in Table 1. For example, a comprehensive study examines the ergodic secrecy achievable rate of an in-home system in the presence of an adjacent malicious wireless device[54]. Subsequently, a separate investigation analyzes the effective secrecy throughput utilizing an experimental dataset[55]. In order to enhance security, a scheme is proposed that incorporates artificial noise to improve the hybrid channel[56]. Furthermore, the research explores the PLS of cooperative relaying PLC systems under the presence of an eavesdropper[57]. To address channel noise, a scheme based on full-duplex communication with artificial noise injection is introduced[58]. Additionally, the research delves into the analysis of secrecy rates for a MIMO system, employing the IBFD jamming technique to secure the transmitted data[59]. The effective secrecy throughput is studied under the scenario of passive colluding wireless eavesdroppers, considering both in-home and broadband PLC systems[60]. Furthermore, PLS in the presence of passive eavesdropping is investigated, taking

Contributions	This work	[54]	[55]	[56]	[57]	[58]	[60]	[61]	[59]	[62]
Log-normal channel model	MK model	✓	✓	✓	✓	✓	✓	✓		✓
Bernoulli–Gaussian impulsive noise	✓							✓		✓
Imperfect CSI	✓		✓	✓	✓			✓	✓	✓
Multi-hop system	✓				✓			✓		
Relay	AF				AF			AF		
Multiple Eves	✓			✓		✓	✓			
Proposing scheme	✓			✓	✓	✓	✓		✓	✓

Table 1. Overview of the existing literature.

into account the impact of Bernoulli–Gaussian impulsive noise[61]. Finally, the study provides a thorough analysis of secrecy rate, secrecy outage probability, and secrecy capacity of a broadband system[62].

To the best of our knowledge, there is currently a research gap regarding relay-aided PLS in the presence of multiple eavesdroppers. Motivated by previous studies on cooperative precoding to enhance channel quality for legitimate users[63–65] and cooperative jamming to impair channel quality for unauthorized users in wireless communication[66–68], we propose a novel cooperative jamming and precoding PLS scheme for IBFD DF relay-aided PLC systems. Unlike other studies assuming perfect channel information[69,70], our proposed approach takes into account imperfect channel information and aims to design the precoding matrices at the legitimate nodes. The objective is to maximize the secrecy rate of AF relay-aided PLC systems with imperfect channel information in the presence of multiple eavesdroppers. To achieve this, we utilize an efficient BCD algorithm to iteratively optimize the precoding matrices. By jointly optimizing these matrices, we aim to enhance the secrecy rate by leveraging the cooperative capabilities of the relay and introducing intentional jamming to disrupt the eavesdroppers' reception. The proposed scheme addresses the challenges posed by multiple eavesdroppers and imperfect channel information, which are critical considerations in practical PLC systems.

To ensure the proposed scheme accurately models real-world power line channels, this paper conducts a characterization of the statistical MIMO PLC channel based on an analysis of a set of experimental field measurements[71]. The analysis takes into account various factors that impact data transfer, including fading effects, multipath propagation, and signal frequency. In addition, the noise in PLC is modeled as Bernoulli–Gaussian impulsive noise[72]. Previous research on PLS has considered different scenarios involving imperfect knowledge of CSI, ranging from passive eavesdroppers with unknown CSI[55–57,61,62] to those with estimation errors[59,73]. We consider a system with globally imperfect channels to provide a more comprehensive and realistic approach. In this scenario, all CSIs are partially known by the legitimate nodes in the PLC system due to channel estimation errors. Furthermore, we extend the study from a single-eavesdropper scenario to a multiple-eavesdropper scenario, considering two types of eavesdropping scenarios: non-colluding and colluding. In the non-colluding scenario, the eavesdroppers operate independently and do not share information, while in the colluding scenario, all eavesdroppers collaborate to intercept the legitimate transmission. Specifically, we investigate the severe colluding case to gain deeper insights into the security performance of the proposed scheme.

The subsequent sections of this paper are organized as follows. "System model" presents a detailed description of the system model. In "Simulation and results", the proposed optimization problem is proved to be solvable by a series of transformations. net section showcases the numerical results obtained from the proposed scheme. Finally, "Conclusion" concludes the findings and provides insights for future research directions.

Notations: To simplify the formulation, we denote $\mathbf{A}\mathbf{A}^H$ as $\mathbf{A}^K$ and the vec($\mathbf{A}$) denotes the vectorization of a matrix A.

System model

We consider a secure transmission system as shown in Figs. 1 and 2, where a source tries to transmit confidential information to legitimate users via an FD relay in the presence of multiple eavesdroppers eavesdropping in different time phases. More specifically, we assume all the eavesdroppers can be divided into two sets by their eavesdropping time. The first one can only eavesdrop on messages in the first time phase and the second one can only eavesdrop messages in the second time phase. Because the relay runs in the full-duplex model, self-interference should be involved. In addition, considering the huge attenuation of signals over long distances in the PLC system, the direct link from the source to the legitimate users can be ignored. In the system, the source(S), the relay(R) and the users(D) are involved N_S, N_R and N_D ports, respectively. Two sets of eavesdroppers are equivalent to two multiple-ports eavesdroppers (E_1 and E_2). Here, both sets of eavesdroppers are equipped with N_E ports.

In the system, channels are described by channel transfer function (CTF) $\mathbf{H}_{ij,k}$ as the matrix of coefficients, where i, j and k denote the transmitter, receiver and transmission time phases, respectively. Note that $\mathbf{H}_{RR,1}$ refers to the self-interference matrix , and $\mathbf{H}_{ij,k}$ stays constant in the transmission process. In this paper, considering the multipath effect, frequency-selective effect, and time delay of power lines, this paper adopts the MK model[71] to model the channel, with channel noise characterized as a Bernoulli–Gaussian pulse noise. Due to the imprecision of channel estimation/feedback and the stealthiness of eavesdroppers, it is challenging for the transmitter

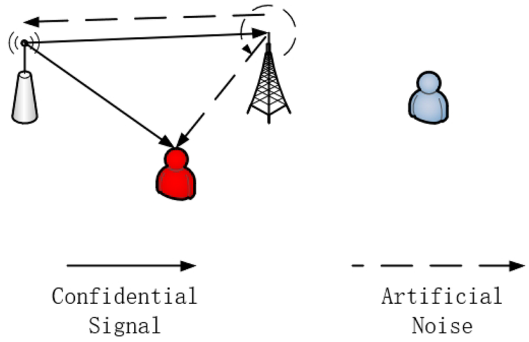

Figure 1. Phase 1 in PLC system.

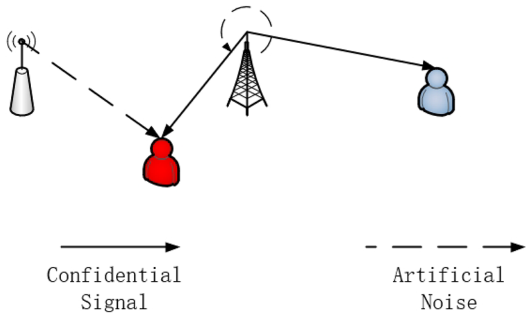

Figure 2. Phase 2 in the PLC system.

to obtain accurate channel state information between the receiver and the transmitter. Therefore, we consider all channels to be imperfect channels.

The imperfect channels are described by the deterministic uncertainty model:

$$\mathbf{H}_{ij,k}\in\mathcal{H}_{ij,k}=\left\{\mathbf{H}_{ij,k}|\mathbf{H}_{ij,k}=\overline{\mathbf{H}}_{ij,k}+\Delta_{ij,k},\left\|\Delta_{ij,k}\right\|\leq\delta_{ij,k}\right\},\tag{1}$$

where $\Delta_{ij,k}$ and $\overline{\mathbf{H}}_{ij,k}$ denote the CTF error and the mean CTF, respectively.

The PLC system is operated over two-time phases with the relay in the AF model. In the two time slots, confidential information is transmitted via a source and a relay. While one of the legitimate nodes propagates the information forward, the other sends jamming signal to deal with possible eavesdroppers. By considering the possible worst-case scenario, the model introduces two groups of eavesdroppers who eavesdrop on two time slots respectively and considers the effect of self-interference at the relay.

In the first time phase, the source broadcasts confidential messages to the relay and the messages are inevitably eavesdropped by E_1. More accurately, the confidential messages are modeled as symbols $\mathbf{S}\in\mathcal{CN}(\mathbf{0},1)$ mapped by vector $\mathbf{W}\in\mathbb{C}^{N_S\times 1}$:

$$\mathbf{X}_s=\mathbf{WS},\tag{2}$$

Next, we consider the messages emitted by the relay which only emits jamming:

$$\mathbf{X}_R=\mathbf{VZ},\tag{3}$$

where $\mathbf{V}\in\mathbb{C}^{N_R\times 1}$ and $\mathbf{Z}\in\mathcal{CN}(\mathbf{0},1)$ denote jamming vector and symbol.

With self-interference, the messages received by the relay can be formulated:

$$\mathbf{Y}_{R1}=\mathbf{H}_{SR,1}\mathbf{WS}+\mathbf{H}_{RR,1}\mathbf{VZ}+\mathbf{n}_{R1},\tag{4}$$

where $\mathbf{n}_{R1}$ is actually PLC noise based on the Bernoulli–Gaussian noise model at the relay.

Meanwhile, E_1 receives the messages from both the source and the relay:

$$\mathbf{Y}_{E1}=\mathbf{H}_{SE,1}\mathbf{WS}+\mathbf{H}_{RE,1}\mathbf{VZ}+\mathbf{n}_{E1},\tag{5}$$

where $\mathbf{n}_{E1}$ is Bernoulli–Gaussian noise at E_1.

In the second time phase, the source emits the jamming precoded from the relay:

$$\mathbf{X}_{S2}=\mathbf{AZ},\tag{6}$$

Meanwhile, the relay is working in the AF mode so it amplifies and forwards the messages it received to both the users and E_2:

$$\mathbf{X}_{R2}=\mathbf{GY}_{R1}=\mathbf{G}(\mathbf{H}_{SR,1}\mathbf{WS}+\mathbf{H}_{RR,1}\mathbf{VZ}+\mathbf{n}_{R1}),\tag{7}$$

where $\mathbf{G}\in\mathbb{C}^{N_R\times N_R}$ denotes the amplifying matrix.

Because of the distance, the jamming from the source will not interrupt users but E_2, i.e.

$$\mathbf{Y}_{E2}=\mathbf{H}_{SE,2}\mathbf{AZ}+\mathbf{H}_{RE,2}\mathbf{G}(\mathbf{H}_{SR,1}\mathbf{WS}+\mathbf{H}_{RR,1}\mathbf{VZ}+\mathbf{n}_{R1})+\mathbf{n}_{E2}\tag{8}$$

$$\mathbf{Y}_D=\mathbf{H}_{RD,2}\mathbf{X}_{R2}+\mathbf{n}_D=\mathbf{H}_{RD,2}\mathbf{G}(\mathbf{H}_{SR,1}\mathbf{WS}+\mathbf{H}_{RR,1}\mathbf{VZ}+\mathbf{n}_{R1})+\mathbf{n}_D,\tag{9}$$

where $\mathbf{n}_D$ is Bernouil–Gaussia noise at the users and $\mathbf{n}_{E2}$ is Bernouil–Gaussia noise at E_2.

Above all, we can calculate the signal-to-noise ratio (SNR) at all the receivers.

$$\gamma_D=(\mathbf{H}_{RD,2}\mathbf{G}\mathbf{H}_{SR,1}\mathbf{W})^K\mathbf{Q}_D^{-1},\quad\text{where}\quad\mathbf{Q}_D=(\mathbf{H}_{RD,2}\mathbf{G}\mathbf{H}_{RR,1}\mathbf{V})^K+\sigma_R^2(\mathbf{H}_{RD,2}\mathbf{G})^K+\sigma_D^2\mathbf{I}\tag{10}$$

$$\gamma_{E1}=(\mathbf{H}_{SE,1}\mathbf{W})^K\mathbf{Q}_{E1}^{-1},\quad\text{where}\quad\mathbf{Q}_{E1}=(\mathbf{H}_{RE,1}\mathbf{V})^K+\sigma_E^2\mathbf{I}\tag{11}$$

$$\gamma_{E2} = (\mathbf{H}_{RE,2}\mathbf{G}\mathbf{H}_{SR,1}\mathbf{W})^K \mathbf{Q}_{E2}^{-1}, \;\; \text{where} \;\; \mathbf{Q}_{E2} = (\mathbf{H}_{SE,2}\mathbf{A})^K + (\mathbf{H}_{RE,2}\mathbf{G}\mathbf{H}_{RR,1}\mathbf{V})^K + \sigma_R^2(\mathbf{H}_{RE,2}\mathbf{G})^K + \sigma_E^2\mathbf{I} \tag{12}$$

and σ_i is the amplitude of the corresponding Bernouil–Gaussia noise $\mathbf{n}_i$.

The achievable rate of the legitimate users is as follows:

$$R_D = \log|\mathbf{I} + \gamma_D|, \tag{13}$$

However, the situation for eavesdropping is more complicated, because the eavesdroppers can collude or not. In the colluding case, the eavesdroppers can utilize maximum ratio combining (MRC) to combine their received information. In this typical collusion strategy, the eavesdropping SNR is the sum of all the eavesdroppers. So the achievable rate of the eavesdroppers is as follows:

$$R_E = \log|\mathbf{I} + \gamma_{E1} + \gamma_{E2}| \tag{14}$$

Jamming precoding scheme

In this work, the goal is to maximize the secrecy rate of the system. With the transmit power constraint, the optimization problem can be formulated as follows.

$$\max_{\mathbf{W},\mathbf{V},\mathbf{A},\mathbf{G}} \; \min_{\mathbf{H}_{ij,k}\in\mathcal{H}_{ij,k}} \; R_D - R_E \tag{15}$$

$$\text{s.t. } \|\mathbf{W}\|^2 \leqslant P_S, \;\; \|\mathbf{A}\|^2 \leqslant P_S, \|\mathbf{V}\|^2 \leqslant P_R, \;\; \mathrm{tr}((\mathbf{G}\mathbf{H}_{SR,1}\mathbf{W})^K + (\mathbf{G}\mathbf{H}_{RR,1}\mathbf{V})^K + \sigma_R^2\mathbf{G}^K) \leqslant P_R \quad \forall \mathbf{H}_{ij,k} \in \mathcal{H}_{ij,k} \tag{16}$$

Because of the high non-convexity of the function $\log|\cdot|$, the problem is hard to solve. To make the problem solvable, (15) is transformed into an equivalent form through WMMSE algorithm, which can be solved with the BCD algorithm. We first introduce WMMSE algorithm.

Lemma1[74]: Define the MSE matrix

$$\widehat{\mathbf{M}} \triangleq (\mathbf{DH}\text{-}\mathbf{I})^K + \mathbf{DRD}^H$$

$$\begin{aligned} -R_E &= \log|\mathbf{Q}| - \log\left|\mathbf{Q} + \mathbf{P}^K\right| \\ &= \log\left|\mathbf{I} + \left[\begin{matrix} \sigma_E^{-2}(\mathbf{H}_{RE,1}\mathbf{V})^K & \mathbf{0} \\ \mathbf{0} & \sigma_E^{-2}[(\mathbf{H}_{SE,2}\mathbf{A})^K + (\mathbf{H}_{RE,2}\mathbf{G}\mathbf{H}_{RR,1}\mathbf{V})^K + \sigma_R^2(\mathbf{H}_{RE,2}\mathbf{G})^K] \end{matrix}\right]\right]\right| \\ &\quad - \log\left|\mathbf{I} + \begin{bmatrix} \sigma_E^{-2}(\mathbf{H}_{RE,1}\mathbf{V})^K & \mathbf{0} \\ \mathbf{0} & \sigma_E^{-2}[(\mathbf{H}_{SE,2}\mathbf{A})^K + (\mathbf{H}_{RE,2}\mathbf{G}\mathbf{H}_{RR,1}\mathbf{V})^K + \sigma_R^2(\mathbf{H}_{RE,2}\mathbf{G})^K] \end{bmatrix} + \begin{bmatrix} \sigma_E^{-1}\mathbf{P}_1 \\ \sigma_E^{-1}\mathbf{P}_2 \end{bmatrix}^K\right| \\ &= \underbrace{\log\left|\mathbf{I} + \sigma_E^{-2}(\mathbf{H}_{RE,1}\mathbf{V})^K\right|}_{C_{E1}} + \underbrace{\log\left|\mathbf{I} + \sigma_E^{-2}[(\mathbf{H}_{SE,2}\mathbf{A})^K + (\mathbf{H}_{RE,2}\mathbf{G}\mathbf{H}_{RR,1}\mathbf{V})^K + \sigma_R^2(\mathbf{H}_{RE,2}\mathbf{G})^K]\right|}_{C_{E2}} \\ &\quad \underbrace{+ - \log\left|\underbrace{\mathbf{I} + \begin{bmatrix} \sigma_E^{-2}(\mathbf{H}_{RE,1}\mathbf{V})^K & \mathbf{0} \\ \mathbf{0} & \sigma_E^{-2}[(\mathbf{H}_{SE,2}\mathbf{A})^K + (\mathbf{H}_{RE,2}\mathbf{G}\mathbf{H}_{RR,1}\mathbf{V})^K + \sigma_R^2(\mathbf{H}_{RE,2}\mathbf{G})^K] \end{bmatrix} + \begin{bmatrix} \sigma_E^{-1}\mathbf{P}_1 \\ \sigma_E^{-1}\mathbf{P}_2 \end{bmatrix}^K}_{\mathbf{M}_{E3}}\right|}_{C_{E3}} \end{aligned} \tag{17}$$

where $\mathbf{R} \succ \mathbf{0}$. Then we have

$$-log|\mathbf{M}| = \max_{\mathbf{S}\succ 0} \; \log|\mathbf{S}| - \mathrm{tr}(\mathbf{SM}) + \mathrm{tr}(\mathbf{I}) \qquad \log\left|\mathbf{I} + \mathbf{R}^{-1}\mathbf{H}^K\right| = \max_{\mathbf{S}\succ 0,\mathbf{D}} \; \log|\mathbf{S}| - \mathrm{tr}(\mathbf{S}\widehat{\mathbf{M}}) + \mathrm{tr}(\mathbf{I}) \tag{18}$$

Furthermore, auxiliary matrices $\mathbf{S}_i, \mathbf{M}_i, \mathbf{D}_i$ are introduced to reformulate the part of $\log|\cdot|$ in the objective function in (15) as follows.

$$R_D = \max_{\mathbf{S}_D\succ 0,\mathbf{D}_D} \; \log|\mathbf{S}_D| - \mathrm{tr}(\mathbf{S}_D\mathbf{M}_D) + \mathrm{tr}(\mathbf{I}) \tag{19}$$

where

$$\mathbf{M}_D = (\mathbf{D}_D\mathbf{H}_{RD,2}\mathbf{G}\mathbf{H}_{SR,1}\mathbf{W} - \mathbf{I})^K + \mathbf{D}_D\mathbf{Q}_D\mathbf{D}_D^H \tag{20}$$

However, (14) is hard to explicit the Lemma1 directly. As a result, we need to transform (14) in a more compatible form.

$$\log|\mathbf{I} + \gamma_{E1} + \gamma_{E2}| = \log\left|\mathbf{I} + \mathbf{P}^K\mathbf{Q}^{-1}\right| \tag{21}$$

where

$$\mathbf{Q} = \begin{bmatrix} \mathbf{Q}_{E1} & \mathbf{0} \\ \mathbf{0} & \mathbf{Q}_{E2} \end{bmatrix}, \mathbf{P} = \begin{bmatrix} \mathbf{P}_1 \\ \mathbf{P}_2 \end{bmatrix} = \begin{bmatrix} \mathbf{H}_{SE,1}\mathbf{W} \\ \mathbf{H}_{RE,2}\mathbf{G}\mathbf{H}_{SR,1}\mathbf{W} \end{bmatrix}$$

Then we have (17), where R_E are divided as C_{E1}, C_{E2} and C_{E3} for subsequent transformation. Thus, in order to formulate the achievable rate of the eavesdroppers in the colluding case, C_{E1} and C_{E2} is equivalent to

$$C_{E1} = \max_{\mathbf{S}_{E1} \succ 0, \mathbf{D}_{E1}} \log|\mathbf{S}_{E1}| - \mathrm{tr}(\mathbf{S}_{E1}\mathbf{M}_{E1}) + \mathrm{tr}(\mathbf{I}) \tag{22}$$

$$C_{E2} = \max_{\mathbf{S}_{E2} \succ 0, \mathbf{D}_{E2}} \log|\mathbf{S}_{E2}| - \mathrm{tr}(\mathbf{S}_{E2}\mathbf{M}_{E2}) + \mathrm{tr}(\mathbf{I}) \tag{23}$$

where

$$\begin{aligned} \mathbf{M}_{E1} &= (\mathbf{D}_{E1}\mathbf{H}_{RE,1}\mathbf{V} - \mathbf{I})^K + \sigma_E^2 \mathbf{D}_{E1}^K \\ \mathbf{M}_{E2} &= (\mathbf{D}_{E21}\mathbf{H}_{SE,2}\mathbf{A}\mathbf{X} + \mathbf{D}_{E22}\mathbf{H}_{RE,2}\mathbf{G}\mathbf{H}_{RR,1}\mathbf{V}\mathbf{X} + \sigma_R \mathbf{D}_{E23}\mathbf{H}_{RE,2}\mathbf{G} - \mathbf{I})^K + \sigma_E^2 \left(\mathbf{D}_{E21}^K + \mathbf{D}_{E22}^K + \mathbf{D}_{E23}^K\right) \end{aligned}$$

$$f \triangleq \log|\mathbf{S}_D| - \mathrm{tr}(\mathbf{S}_D\mathbf{M}_D) + \log|\mathbf{S}_{E1}| - \mathrm{tr}(\mathbf{S}_{E1}\mathbf{M}_{E1}) + \log|\mathbf{S}_{E2}| - \mathrm{tr}(\mathbf{S}_{E2}\mathbf{M}_{E2}) + \log|\mathbf{S}_{E3}| - \mathbf{tr}(\mathbf{S}_{E3}\mathbf{M}_{E3}) \tag{24}$$

$$g \triangleq \log|\mathbf{S}_D| - \beta_D + \log|\mathbf{S}_{E1}| - \beta_{E1} + \log|\mathbf{S}_{E2}| - \beta_{E2} + \log|\mathbf{S}_{E3}| - \beta_{E3} \tag{25}$$

Note the decomposition $\mathbf{D}_{E2} = \begin{bmatrix} \mathbf{D}_{E21} & \mathbf{D}_{E22} & \mathbf{D}_{E23} \end{bmatrix}$ and $\mathbf{X} = \begin{bmatrix} 1 & \mathbf{0} \end{bmatrix} \in \mathbb{C}^{1 \times N_R}$.
Then to solve C_{E3}, we also apply Lemma1 :

$$C_{E3} = \max_{\mathbf{S}_{E3} \succ 0} \log|\mathbf{S}_{E3}| - \mathbf{tr}(\mathbf{S}_{E3}\mathbf{M}_{E3}) + \mathbf{tr}(\mathbf{I}) \tag{26}$$

After substituting (22)–(26) into (15), the secrecy rate of the system with the colluding eavesdroppers can be rewritten as

$$\max_{\mathbf{W},\mathbf{V},\mathbf{A},\mathbf{G},\mathbf{S}_i \succ 0, \mathbf{D}_i} \; \min_{\mathbf{H}_{ij,k} \in \mathcal{H}_{ij,k}} f(\mathbf{W},\mathbf{V},\mathbf{A},\mathbf{G},\mathbf{S_i},\mathbf{D_i}), \quad \text{s.t.}(16) \tag{27}$$

where $f(\mathbf{W},\mathbf{V},\mathbf{A},\mathbf{G},\mathbf{S_i},\mathbf{D_i})$ is defined in (24).

The max-min problem and constrain $\mathrm{tr}((\mathbf{G}\mathbf{H}_{SR,1}\mathbf{W})^K + (\mathbf{G}\mathbf{H}_{RR,1}\mathbf{V})^K + \sigma_R^2\mathbf{G}^K) \le P_R$ can be transformed into an optimization problem by introducing constraints with slack variables β_i as follows.

$$\mathrm{tr}(\mathbf{S}_i\mathbf{M}_i) \le \beta_i, \forall \mathbf{H}_{ij,k} \in \mathcal{H}_{ij,k} \tag{28}$$

The problem (27) can be further transformed as

$$\max_{\mathbf{W},\mathbf{V},\mathbf{A},\mathbf{G},\mathbf{S}_i \succ 0, \mathbf{D}_i} g(\mathbf{W},\mathbf{V},\mathbf{A},\mathbf{G},\mathbf{S_i},\mathbf{D_i}), \quad \text{s.t.}(16), \;(26) \tag{29}$$

where $g(\mathbf{W},\mathbf{V},\mathbf{A},\mathbf{G},\mathbf{S_i},\mathbf{D_i})$ is defined in (25).

However, (25) is still convex because of the semi-infinite constraints (28). For $i = D$, $\mathrm{tr}(\mathbf{S}_D\mathbf{M}_D)$ can be rewritten as

$$\mathrm{tr}(\mathbf{S}_D\mathbf{M}_D) = \left\| \underbrace{\begin{bmatrix} \mathrm{vec}(\mathbf{F}_D(\mathbf{D}_D\mathbf{H}_{RD,2}\mathbf{G}\mathbf{H}_{SR,1}\mathbf{W} - \mathbf{I})) \\ \mathrm{vec}(\mathbf{F}_D\mathbf{D}_D\mathbf{H}_{RD,2}\mathbf{G}\mathbf{H}_{RR,1}\mathbf{V}) \\ \mathrm{vec}(\sigma_R\mathbf{F}_D\mathbf{D}_D\mathbf{H}_{RD,2}\mathbf{G}) \\ \mathrm{vec}(\sigma_D\mathbf{F}_D\mathbf{D}_D) \end{bmatrix}}_{\phi_D} \right\|^2 \tag{30}$$

where $\mathbf{S}_D = \mathbf{F}_D^H\mathbf{F}_D$ and the equality $\mathrm{tr}(\mathbf{A}^K) = \|\mathrm{vec}(\mathbf{A})\|^2$ is applied.

Especially note that for $i = E3$, to obtain similiar form as (30), $\mathbf{F}_{E3}$ should be divided as

$$\mathbf{F}_{E3} = \begin{bmatrix} \mathbf{F}_{E31} & \mathbf{F}_{E32} \end{bmatrix}, \;\; \mathbf{F}_{E31}, \mathbf{F}_{E32} \in \mathbb{C}^{2N_E \times N_E} \tag{31}$$

So we have

$$\mathrm{tr}(\mathbf{S}_{E3}\mathbf{M}_{E3}) = \left\| \begin{matrix} \mathrm{vec}(\mathbf{F}_{E31}) \\ \mathrm{vec}(\mathbf{F}_{E32}) \\ \mathrm{vec}(\sigma_E^{-1}\mathbf{F}_{E31}\mathbf{H}_{RE,1}\mathbf{V}) \\ \mathrm{vec}(\sigma_E^{-1}\mathbf{F}_{E32}\mathbf{H}_{SE,2}\mathbf{A}) \\ \mathrm{vec}(\sigma_E^{-1}\mathbf{F}_{E32}\mathbf{H}_{RE,2}\mathbf{G}\mathbf{H}_{RR,1}\mathbf{V}) \\ \mathrm{vec}(\sigma_E^{-1}\sigma_R\mathbf{F}_{E32}\mathbf{H}_{RE,2}\mathbf{G}) \\ \mathrm{vec}(\sigma_E^{-1}\mathbf{F}_{E31}\mathbf{H}_{SE,1}\mathbf{W}) \\ \mathrm{vec}(\sigma_E^{-1}\mathbf{F}_{E32}\mathbf{H}_{RE,2}\mathbf{G}\mathbf{H}_{SR,1}\mathbf{W}) \end{matrix} \right\|^2 \tag{32}$$

Focusing on the uncertain CTF, (30) can be rewritten as follows.

$$\phi_D = \bar{\phi}_D + \underbrace{\sum_j \mathbf{\Omega}_{Dj}\mathrm{vec}(\Delta_j)}_{\Delta_D} + \underbrace{\sum_k \alpha_k \mathrm{vec}(\Delta_{k1})\mathrm{vec}^H(\Delta_{k2})}_{\widetilde{\Delta}_D} \tag{33}$$

where the identity $\mathrm{vec}(\mathbf{ABC}) = \left(\mathbf{C}^T \otimes \mathbf{A}\right)\mathrm{vec}(\mathbf{B})$ is applied. Δ_D and $\widetilde{\Delta}_D$ is the linear part and the quadratic part of the CTF uncertainty, respectively. Actually the quadratic part is negligible. Then, we only consider asymptotic form of ϕ_D as

$$\phi_D = \bar{\phi}_D + \underbrace{\sum_j \mathbf{\Omega}_{Dj}\mathrm{vec}(\Delta_j)}_{\Delta_D} \tag{34}$$

where

$$\mathbf{\Omega}_{DSR,1} = \begin{bmatrix} \mathbf{W}^T \otimes \mathbf{F}_D\mathbf{D}_D\overline{\mathbf{H}}_{RD,2}\mathbf{G} \\ \mathbf{0} \\ \mathbf{0} \\ \mathbf{0} \end{bmatrix}, \mathbf{\Omega}_{DSD,2} = \begin{bmatrix} (\mathbf{G}\overline{\mathbf{H}}_{SR,1}\mathbf{W})^T \otimes \mathbf{F}_D\mathbf{D}_D \\ (\mathbf{G}\overline{\mathbf{H}}_{RR,1}\mathbf{V})^T \otimes \mathbf{F}_D\mathbf{D}_D \\ \sigma_R\mathbf{G}^T \otimes \mathbf{F}_D\mathbf{D}_D \\ \mathbf{0} \end{bmatrix}, \mathbf{\Omega}_{DRR,1} = \begin{bmatrix} \mathbf{0} \\ \mathbf{V}^T \otimes \mathbf{F}_D\mathbf{D}_D\overline{\mathbf{H}}_{RD,2}\mathbf{G} \\ \mathbf{0} \\ \mathbf{0} \end{bmatrix} \tag{35}$$

For other situations and for the constraint $\mathrm{tr}((\mathbf{GH}_{SR,1}\mathbf{W})^K + (\mathbf{GH}_{RR,1}\mathbf{V})^K + \sigma_R^2\mathbf{G}^K) \leq P_R$, similiar formulas can be obtained through the same method. While the power constraint does not involve any quadratic part of the CTF uncertainty, so the original problem constraints are not relaxed.

With (30) and (34) and by exploiting the Schur complement lemma[75], (28) can be rewritten as matrix inequality .

$$\begin{bmatrix} \beta_D & \bar{\phi}_D^H \\ \bar{\phi}_D & \mathbf{I} \end{bmatrix} \succ - \begin{bmatrix} 0 & \mathit{\Delta}_D^H \\ \mathit{\Delta}_D & \mathbf{0} \end{bmatrix} \tag{36}$$

The constraint (36) still contains the uncertainty Δ_D. The sign-definiteness lemma is applied to eliminate this uncertainty.

Lemma 2[76]: Given a Hermitian matrix $\mathbf{A}$ and arbitrary matrices pair $\{\mathbf{P}_i, \mathbf{Q}_i\}$, $i \in \{1, 2, \ldots, N\}$, the semi-infinite Linear Matrix Inequality (LMI)

$$\mathbf{A} \succ \sum_i^N \left(\mathbf{P}_i^H\mathbf{Y}_i\mathbf{Q}_i + \mathbf{Q}_i^H\mathbf{Y}_i^H\mathbf{P}_i\right), \ \|\mathbf{Y}_i\| \leq \delta_i \tag{37}$$

holds if and only if there exist nonnegative real numbers $\lambda_1, \lambda_2, \ldots, \lambda_N$ such that

$$\begin{bmatrix} \mathbf{A} - \sum_{i=1}^N \lambda_i\mathbf{Q}_i^H\mathbf{Q}_i & -\delta_1\mathbf{P}_1^H & \cdots & -\delta_N\mathbf{P}_N^H \\ -\delta_1\mathbf{P}_1 & \delta_1\mathbf{I} & \cdots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ -\delta_N\mathbf{P}_N & \mathbf{0} & \cdots & \delta_N\mathbf{I} \end{bmatrix} \succ \mathbf{0} \tag{38}$$

$$h \triangleq 2\log|\mathbf{F}_D| - \beta_D + 2\log|\mathbf{F}_{E1}| - \beta_{E1} + 2\log|\mathbf{F}_{E2}| - \beta_{E2} + 2\log|\mathbf{F}_{E3}| - \beta_{E3} \tag{39}$$

Appropriately choose the parameters as below

$$\mathbf{A}_D = \begin{bmatrix} \beta_D & \bar{\phi}_D^H \\ \bar{\phi}_D & \mathbf{I} \end{bmatrix}, \mathbf{Q}_{D1}, \mathbf{Q}_{D2}, \mathbf{Q}_{D3} = [-\mathbf{10}], \mathbf{P}_{D1} = \begin{bmatrix} \mathbf{0} & \mathbf{\Omega}_{DSR,1}^H \end{bmatrix}, \mathbf{P}_{D2} = \begin{bmatrix} \mathbf{0} & \mathbf{\Omega}_{DSD,2}^H \end{bmatrix}, \mathbf{P}_{D3} = \begin{bmatrix} \mathbf{0} & \mathbf{\Omega}_{DRR,1}^H \end{bmatrix} \tag{40}$$

Apply lemma 2 and insert (40) to (36) , and we have

$$\begin{bmatrix} \begin{bmatrix} \beta_D - \lambda_{D1} - \lambda_{D2} - \lambda_{D3} & \bar{\phi}_D^H \\ \bar{\phi}_D & \mathbf{I} \end{bmatrix} & \theta_D^H \\ \theta_D & \mathrm{diag}(\lambda_{D1}\mathbf{I}, \lambda_{D2}\mathbf{I}, \lambda_{D3}\mathbf{I}) \end{bmatrix} \succ 0 \tag{41}$$

where $\theta_D = -[\delta_{DSR,1}\mathbf{P}_{D1}^T, \delta_{DSD,2}\mathbf{P}_{D2}^T, \delta_{DRR,1}\mathbf{P}_{D3}^T]^T$. Similarly, other inequalities $\mathrm{tr}(\mathbf{S}_i\mathbf{M}_i) \leq \beta_i$ can be transfered into the same form as following.

$$\begin{bmatrix} \begin{bmatrix} \beta_i - \sum_{k=l}^j \lambda_k & \bar{\phi}_i^H \\ \bar{\phi}_i & \mathbf{I} \end{bmatrix} & \theta_i^H \\ \theta_i & \left[\lambda_l\mathbf{I}, \cdots, \lambda_j\mathbf{I}\right] \end{bmatrix} \succ 0 \tag{42}$$

With all components, the problem is equivalent to

$$\max_{\mathbf{W},\mathbf{V},\mathbf{A},\mathbf{G},\mathbf{F}_i\succ 0,\mathbf{D}_i,\lambda_i\geq 0,\beta_i} h(\mathbf{W},\mathbf{V},\mathbf{A},\mathbf{G},\mathbf{F_i},\mathbf{D_i},\lambda_i,\beta_i), \quad \text{s.t. } (16),\ (40),\ (41) \tag{43}$$

where the function $h(\mathbf{W},\mathbf{V},\mathbf{A},\mathbf{G},\mathbf{F_i},\mathbf{D_i},\lambda_i,\beta_i)$ is defined in (39).

Although (43) is still non-convex. However, it is convex with respective to $\mathbf{F}_i$ or any one in $\mathbf{W},\mathbf{V},\mathbf{A},\mathbf{G},\mathbf{D_i}$. As a result, (43) can be solved via BCD algorithm as below.

```
set $l$= 0, $\mathbf{W}$=$\mathbf{W}^{(0)}$, $\mathbf{V}$=$\mathbf{V}^{(0)}$, $\mathbf{A}$=$\mathbf{A}^{(0)}$, $\mathbf{F}_i = \mathbf{F}_i^{(0)}$, $\mathbf{G} = \mathbf{G}^{(0)}$and an accuracy parameter $\varepsilon$;
repeat
  1:Solve (42) to update $\mathbf{D}_i$ with other parameters fixed;
  2:Solve (42) to update $\mathbf{F}_i$ with other fixed parameters which are found in previous steps;
  3:Solve (42) to update $\mathbf{W},\mathbf{V},\mathbf{A}$ with other fixed parameters which are found in previous steps;
  4:Solve (42) to update $\mathbf{G}$ with other fixed parameters which are found in previous steps;
until $\left|y^{(i)} - y^{(i-1)}\right| \leq \varepsilon$,where $y^{(i)}$ denotes optimum value of (42) in $i$th iteration
```

Algorithm 1. Jamming precoding scheme to solve problem (43).

The variables to be optimized in the optimization problem are divided into the following groups.

$$\Phi_0 = \{\lambda_i,\beta_i\}, \Phi_1 = \{\mathbf{D}_i,\Phi_0\}, \Phi_2 = \{\mathbf{F}_i,\Phi_0\}, \Phi_3 = \{\mathbf{W},\mathbf{V},\mathbf{A},\Phi_0,\}, \Phi_4 = \{\mathbf{G},\Phi_0\} \tag{44}$$

By optimizing the problem in order $\Phi_1 \to \Phi_2 \to \Phi_3 \to \Phi_4$, we denote $y_k^{(i)}$ as the optimal value optimized to Φ_k in the ith iteration. Since the variables to be optimized always meet the constraints in the optimization process, the optimal value will not decrease :

$$y^{(i)} = y_4^{(i)} \geq y_3^{(i)} \geq y_2^{(i)} \geq y_1^{(i)} \geq y^{(i-1)} = y_4^{(i-1)} \geq y_3^{(i-1)} \geq y_2^{(i-1)} \geq y_1^{(i-1)} \cdots \tag{45}$$

Obviously with constraints (16), the secrecy rate is bounded and the objective function value increases in each iteration, which proves the convergence.

Simulation and results

In the simulation parts, the statistical MIMO PLC channels are generated by formula (1) in reference[71], and the specific parameters are shown in Table 2. And the noises in PLC are also modeled as a Bernoulli–Gaussian impulsive noise.

In this section, numerical results are presented to prove the effectiveness of precoding jamming scheme in terms of average secrecy rate. In this part, without specific definition, we consider $N_S = N_R = N_D = N_E = N = 2$. Besides, for the simplicity, the CTF uncertanity bound $\delta_{ij,k}$ are related to corresponding determinant of mean CTF with one certain coefficient, or $\delta_{ij,k} = \mu\left\|\overline{\mathbf{H}_{ij,k}}\right\|$. Apparently, it accords with the natural assumption that CTF with larger determinant tends to be more uncertain.

Figures 3 and 4 illustrate the relationship between the average secrecy rate and the number of iterations, assuming power constraints $P_S = P_R = P = 10\,\text{dB}$. Notably, the average secrecy rate consistently stabilizes after approximately 40 iterations. This indicates that heightened CTF uncertainty detrimentally impacts the secrecy rate. Moreover, the proposed approach exhibits superior performance with an increased number of legitimate user ports and a reduced number of eavesdropper ports. This distinction becomes particularly pronounced in scenarios characterized by larger CTF uncertainty. In essence, the number of ports directly correlates with the capacity for receiving or intercepting information.

We examine the characteristics of the proposed scheme under varying transmit power levels in Figs. 5 and 6. The analysis reveals an increase in the average secrecy rate as the transmit power is raised. However, beyond a

Path loss parameter	Model	Parameters
$A_{\text{dB } S1,D1}$	$\mathcal{N}(\mu_A,\sigma_A)$	$\mu_A = -50.1$ dB $\sigma_A = 15.6$ dB
$A_{\text{dB } Sm,Dn}$ $m \in [1,2,3]$	$A_{\text{dB } Sm,Dn} = A_{\text{dB } S1,D1} + \mathcal{N}(0,\sigma_{Sm,Dn})$	$[\sigma_{Sm},Dn] = \begin{bmatrix} 0 & 5.1 & 3.8 \\ 2.9 & 5.7 & 5.2 \\ 6.6 & 7.8 & 6.9 \\ 4.6 & 5.9 & 5.1 \end{bmatrix}$ dB
$A_{\text{dB S4,Dn}}$	$A_{\text{dB } S4,Dn} = 0.5 \times A_{\text{dB } S1,D1} - 30 + \mathcal{N}(0,\sigma_{S4,Dn})$	
a_0	$E_{\text{shift}}(\mu_{a_0},\delta_{a_0})$	$\mu_{a_0} = 1.04 \times 10^{-2}$ $\delta_{a_0} = -6.7 \times 10^{-3}$
a_1	Constant	$a_1 = 4 \times 10^{-10}$
K	$\mathcal{W}(\alpha_K,\beta_K)$	$\alpha_K = 5.7 \times 10^{-2}$ $\beta_K = 57.7$
L_{max}	Constant	$L_{max} = 800\,\text{m}$
Λ	Constant	$\Lambda = 0.2\,\text{m}^{-1}$

Table 2. Parameters of the PLC channels[71].

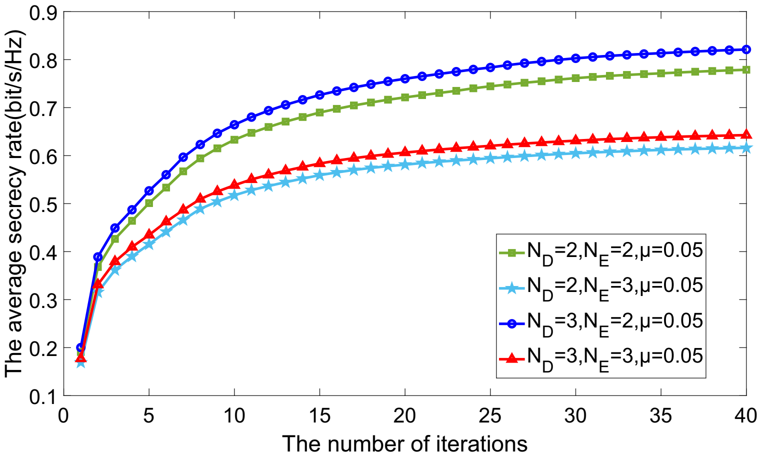

Figure 3. Average secrecy rate versus numbers of iterations comparison of different ports number and CTF uncertainty.

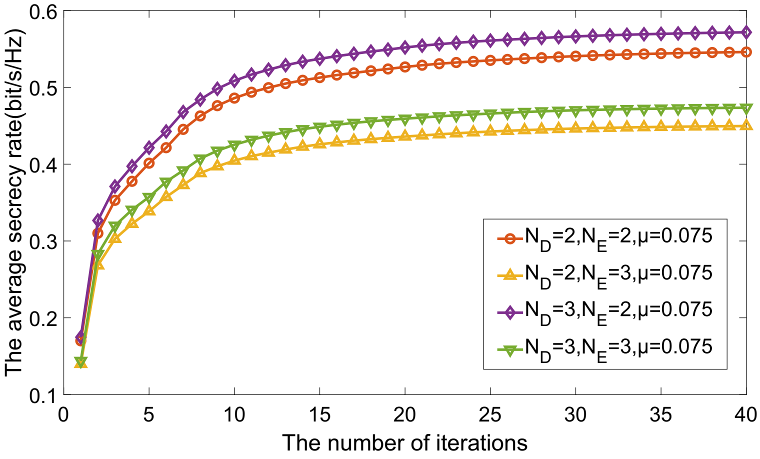

Figure 4. Average secrecy rate versus numbers of iterations comparison of different ports number and CTF uncertainty.

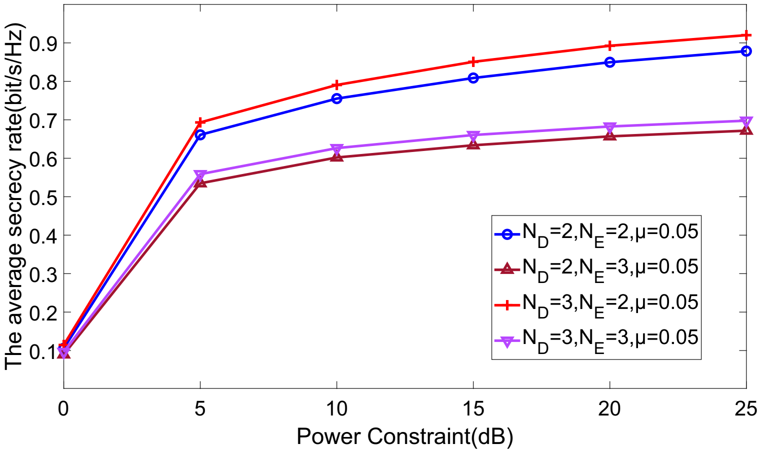

Figure 5. Average secrecy rate versus power constraint comparison of different ports number and CTF uncertainty.

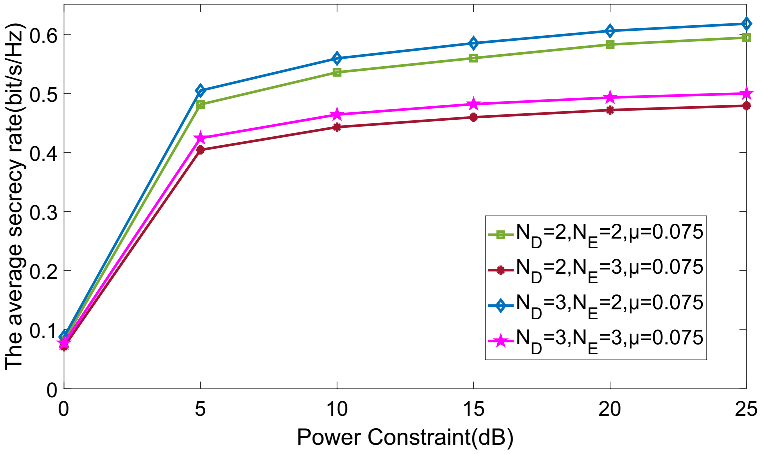

Figure 6. Average secrecy rate versus power constraint comparison of different ports number and CTF uncertainty.

transmission power of 10 dB, especially in scenarios with more eavesdropper ports and increased CTF uncertainty, the secrecy rate experiences only marginal improvement. This is attributed to the fact that elevating transmit power enhances not only the capacity of legitimate users but also that of eavesdroppers colluding to boost their eavesdropping rate. Consequently, this simultaneous enhancement leads to only a slight alteration in the overall secrecy rate. Additionally, when the numbers of legitimate user ports and eavesdropper ports both increase from 2 to 3, there is a notable decrease in the average secrecy rate. This observation suggests that in collusion scenarios, the expansion of the eavesdroppers' port number has a more substantial impact on the PLC system than the growth in the number of legitimate users' ports.

We assess the influence of jamming by showcasing the numerical outcomes of our proposed schemes alongside a comparable one lacking jamming signals in Fig. 7. This figure shows improvements achieved by the proposed algorithm compared to the traditional one. As shown in Fig. 7, the proposed algorithm achieves higher secure rates than the traditional algorithm when $\mu = 0.05$ or $\mu = 0.075$, and the advantage increases with increasing power. Specifically, when $\mu = 0.05$ and the transmission power is 20 dB, the secure rate of the proposed algorithm can reach 0.85 bit/s/Hz, while the traditional algorithm achieves 0.61 bit/s/Hz. In contrast to the jamming-free scheme, our proposed approach demonstrates superior performance, particularly regarding the average secrecy rate, especially under conditions of lower CTF uncertainty and increased transmit power. This suggests that, to a certain degree, jamming has the capability to disrupt the interception efforts of eavesdroppers, even in scenarios characterized by higher CTF uncertainty.

Figure 8 depicts how the ports of eavesdroppers affect the PLC system, where $N_S = N_R = N_D = 2$. It suggests the ability of eavesdroppers increases with the growth of their ports, especially in few ports.

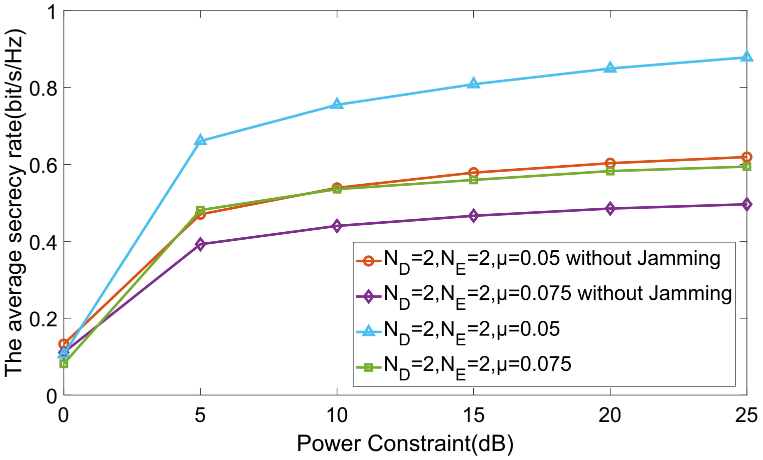

Figure 7. Average secrecy rate versus power constraint comparison of different schemes.

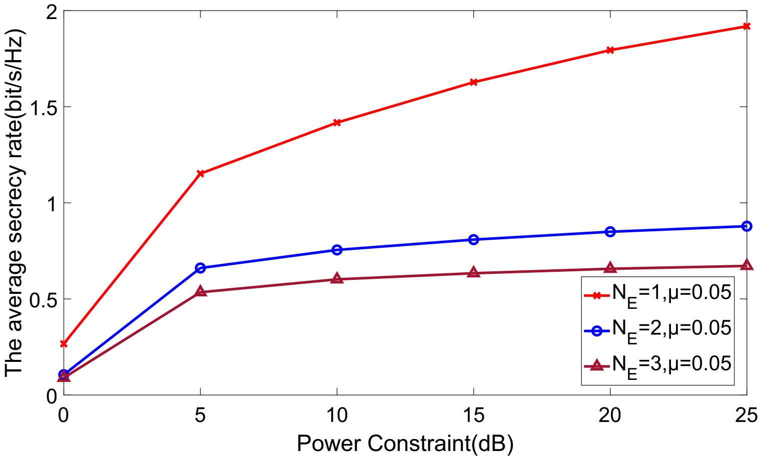

Figure 8. Average secrecy rate versus different eavesdropping ports number.

Conclusion

The paper introduces a precoding jamming scheme aimed at bolstering the security of AF relay-aided PLC systems when faced with the challenge of multiple colluding eavesdroppers, while also considering CTF uncertainty. The numerical results unequivocally establish the superiority of our proposed scheme compared to a jamming-free alternative. Notably, the effectiveness of the proposed scheme is underscored, especially in scenarios characterized by elevated CTF uncertainty.

Data availability

The datasets generated and/or analysed during the current study are available in the github repository, https://github.com/zilongmi/Jamming-Precoding-in-AF-Relay-aided-PLC-Systems-with-Multiple-Eavessdroppers.

Received: 21 November 2023; Accepted: 2 April 2024
Published online: 09 April 2024

References

1. Ferreira, H. C., Lampe, L., Newbury, J. & Swart, T. G. *Power Line Communications: Theory and Applications for Narrowband and Broadband Communications Over Power Lines* (Wiley, 2011).
2. Lallbeeharry, N., Mazari, R., Dégardin, V. & Trebosc, C. Plc applied to fault detection on in-vehicle power line. In *2018 IEEE International Symposium on Power Line Communications and its Applications (ISPLC)*, 1–5. https://doi.org/10.1109/ISPLC.2018.8360233 (2018).
3. Camponogara, Oliveira, T. R., Machado, R., Finamore, W. A. & Ribeiro, M. V. Measurement and characterization of power lines of aircraft flight test instrumentation. *IEEE Trans. Aerosp. Electron. Syst.* **55**, 1550–1560. https://doi.org/10.1109/TAES.2019.2913613 (2019).
4. Dickmann, G. DigitalSTROM®: A centralized plc topology for home automation and energy management. In *2011 IEEE International Symposium on Power Line Communications and Its Applications*, 352–357 (IEEE, 2011).
5. Sendin, A., Simon, J., Urrutia, I. & Berganza, I. PLC deployment and architecture for Smart Grid applications in Iberdrola. In *18th IEEE International Symposium on Power Line Communications and Its Applications*, 173–178 (IEEE, 2014).
6. Sendin, A., Berganza, I., Arzuaga, A., Pulkkinen, A. & Kim, I. H. Performance results from 100,000+ PRIME smart meters deployment in Spain. In *2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*, 145–150 (IEEE, 2012).
7. Goedhart, A., Heymann, R. & Ferreira, H. Adapting HomePlug C &C PLC for use in a low voltage smart grid. In *2012 IEEE International Symposium on Power Line Communications and Its Applications*, 194–199 (IEEE, 2012).
8. Mlynek, P., Koutny, M., Misurec, J. & Kolka, Z. Measurements and evaluation of PLC modem with G3 and PRIME standards for Street Lighting Control. In *18th IEEE International Symposium on Power Line Communications and Its Applications*, 238–243 (IEEE, 2014).
9. Castor, L. R., Natale, R., Silva, J. A. & Segatto, M. E. Experimental investigation of broadband power line communication modems for onshore oil and gas industry: A preliminary analysis. In *18th IEEE International Symposium on Power Line Communications and Its Applications*, 244–248 (IEEE, 2014).
10. Degauque, P. *et al.* Power-line communication: Channel characterization and modeling for transportation systems. *IEEE Veh. Technol. Mag.* **10**, 28–37 (2015).
11. Pittolo, A., De Piante, M., Versolatto, F. & Tonello, A. M. In-vehicle power line communication: Differences and similarities among the in-car and the in-ship scenarios. *IEEE Veh. Technol. Mag.* **11**, 43–51 (2016).
12. Degardin, V. *et al.* On the possibility of using PLC in aircraft. In *ISPLC2010*, 337–340 (IEEE, 2010).
13. Antoniali, M., Tonello, A. M., Lenardon, M. & Qualizza, A. Measurements and analysis of PLC channels in a cruise ship. In *2011 IEEE International Symposium on Power Line Communications and Its Applications*, 102–107 (IEEE, 2011).
14. Barmada, S., Bellanti, L., Raugi, M. & Tucci, M. Analysis of power-line communication channels in ships. *IEEE Trans. Veh. Technol.* **59**, 3161–3170 (2010).
15. Barmada, S. *et al.* Design of a PLC system onboard trains: Selection and analysis of the PLC channel. In *2008 IEEE International Symposium on Power Line Communications and Its Applications*, 13–17 (IEEE, 2008).
16. Facina, M. S. P., Latchman, H. A., Poor, H. V. & Ribeiro, M. V. Cooperative in-home power line communication: Analyses based on a measurement campaign. *IEEE Trans. Commun.* **64**, 778–789. https://doi.org/10.1109/TCOMM.2015.2499744 (2016).

17. Cataliotti, A., Cosentino, V., Di Cara, D. & Tinè, G. Measurement issues for the characterization of medium voltage grids communications. *IEEE Trans. Instrum. Meas.* **62**, 2185–2196. https://doi.org/10.1109/TIM.2013.2264861 (2013).
18. Huang, G., Akopian, D. & Chen, C. L. P. Measurement and characterization of channel delays for broadband power line communications. *IEEE Trans. Instrum. Meas.* **63**, 2583–2590. https://doi.org/10.1109/TIM.2014.2313033 (2014).
19. Janse van Rensburg, P. A. & Ferreira, H. C. Coupler winding ratio selection for effective narrowband power-line communications. *IEEE Trans. Power Deliv.* **23**, 140–149. https://doi.org/10.1109/TPWRD.2007.905790 (2008).
20. Kirik, M. & Hamamreh, J. M. Interference signal superposition-aided MIMO with antenna number modulation and adaptive antenna selection for achieving perfect secrecy. *RS Open J. Innov. Commun. Technol.***2** (2021). https://rs-ojict.pubpub.org/pub/m2jdsq52.
21. Lemayian, J. P. & Hamamreh, J. M. Physical layer security analysis of hybrid MIMO technology. *RS Open J. Innov. Commun. Technol.***2** (2021). https://rs-ojict.pubpub.org/pub/1v7f9gfb.
22. Hong, Y.-W.P., Huang, W.-J. & Kuo, C.-C.J. *Cooperative Communications and Networking: Technologies and System Design* (Springer, 2010).
23. Yoon, S.-G., Jang, S., Kim, Y.-H. & Bahk, S. Opportunistic routing for smart grid with power line communication access networks. *IEEE Trans. Smart Grid* **5**, 303–311. https://doi.org/10.1109/TSG.2013.2279184 (2014).
24. Cheng, X., Cao, R. & Yang, L. Relay-aided amplify-and-forward powerline communications. *IEEE Trans. Smart Grid* **4**, 265–272. https://doi.org/10.1109/TSG.2012.2225645 (2013).
25. Lampe, L., Schober, R. & Yiu, S. Distributed space-time coding for multihop transmission in power line communication networks. *IEEE J. Sel. Areas Commun.* **24**, 1389–1400. https://doi.org/10.1109/JSAC.2006.874419 (2006).
26. Balakirsky, V. & Han Vinck, A. Potential performance of plc systems composed of several communication links. In *International Symposium on Power Line Communications and Its Applications, 2005*, 12–16. https://doi.org/10.1109/ISPLC.2005.1430456 (2005).
27. Prasad, G., Lampe, L. & Shekhar, S. In-band full duplex broadband power line communications. *IEEE Trans. Commun.* **64**, 3915–3931. https://doi.org/10.1109/TCOMM.2016.2587284 (2016).
28. Riihonen, T., Werner, S. & Wichman, R. Optimized gain control for single-frequency relaying with loop interference. *IEEE Trans. Wirel. Commun.* **8**, 2801–2806. https://doi.org/10.1109/TWC.2009.080542 (2009).
29. Riihonen, T., Werner, S. & Wichman, R. Hybrid full-duplex/half-duplex relaying with transmit power adaptation. *IEEE Trans. Wirel. Commun.* **10**, 3074–3085. https://doi.org/10.1109/TWC.2011.071411.102266 (2011).
30. Kang, Y. Y., Kwak, B.-J. & Cho, J. H. An optimal full-duplex af relay for joint analog and digital domain self-interference cancellation. *IEEE Trans. Commun.* **62**, 2758–2772. https://doi.org/10.1109/TCOMM.2014.2342230 (2014).
31. Li, S. *et al.* Full-duplex amplify-and-forward relaying: Power and location optimization. *IEEE Trans. Veh. Technol.* **66**, 8458–8468. https://doi.org/10.1109/TVT.2017.2686872 (2017).
32. Sabharwal, A. *et al.* In-band full-duplex wireless: Challenges and opportunities. *IEEE J. Sel. Areas Commun.* **32**, 1637–1652. https://doi.org/10.1109/JSAC.2014.2330193 (2014).
33. Choi, Y.-S. & Shirani-Mehr, H. Simultaneous transmission and reception: Algorithm, design and system level performance. *IEEE Trans. Wirel. Commun.* **12**, 5992–6010. https://doi.org/10.1109/TWC.2013.101713.121152 (2013).
34. Cañete, F. J., Prasad, G. & Lampe, L. Plc networks with in-band full-duplex relays. In *2020 IEEE International Symposium on Power Line Communications and its Applications (ISPLC)*, 1–6. https://doi.org/10.1109/ISPLC48789.2020.9115410 (2020).
35. Kim, D., Lee, H. & Hong, D. A survey of in-band full-duplex transmission: From the perspective of phy and mac layers. *IEEE Commun. Surv. Tutor.* **17**, 2017–2046. https://doi.org/10.1109/COMST.2015.2403614 (2015).
36. Rothe, S. *et al.* Physical layer security in multimode fiber optical networks. *Sci. Rep.* **10**, 2740 (2020).
37. Barbeau, M. & Garcia-Alfaro, J. Cyber-physical defense in the quantum era. *Sci. Rep.* **12**, 1905 (2022).
38. Abewa, M. & Hamamreh, J. M. Multi-user auxiliary signal superposition transmission (MU-AS-ST) for secure and low-complexity multiple access communications. *RS Open J. Innov. Commun. Technol.***2** (2021). https://rs-ojict.pubpub.org/pub/qiuo9m8s.
39. Lemayian, J. P. & Hamamreh, J. M. A novel small-scale nonorthogonal communication technique using auxiliary signal superposition with enhanced security for future wireless networks. *RS Open Journal on Innovative Communication Technologies***1** (2020). Https://rs-ojict.pubpub.org/pub/rd8elz19.
40. Anastasiadou, D. & Antonakopoulos, T. Multipath characterization of indoor power-line networks. *IEEE Trans. Power Deliv.* **20**, 90–99. https://doi.org/10.1109/TPWRD.2004.832373 (2005).
41. Zimmermann, M. & Dostert, K. A multipath model for the powerline channel. *IEEE Trans. Commun.* **50**, 553–559. https://doi.org/10.1109/26.996069 (2002).
42. Schwager, A., Schneider, D., Bäschlin, W., Dilly, A. & Speidel, J. Mimo plc: Theory, measurements and system setup. In *2011 IEEE International Symposium on Power Line Communications and Its Applications*, 48–53. https://doi.org/10.1109/ISPLC.2011.5764447 (2011).
43. Hamamreh, J., Furqan, M. & Arslan, H. Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey. *IEEE Commun. Surv. Tutor.*https://doi.org/10.1109/COMST.2018.2878035 *(2018).*
44. Wyner, A. D. The wire-tap channel. *Bell Syst. Tech. J.* **54**, 1355–1387 (1975).
45. Leung-Yan-Cheong, S. & Hellman, M. The gaussian wire-tap channel. *IEEE Trans. Inf. Theory* **24**, 451–456 (1978).
46. Csiszar, I. & Korner, J. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory* **24**, 339–348. https://doi.org/10.1109/TIT.1978.1055892 (1978).
47. Parada, P. & Blahut, R. Secrecy capacity of simo and slow fading channels. In *Proceedings. International Symposium on Information Theory, 2005. ISIT 2005*, 2152–2155. https://doi.org/10.1109/ISIT.2005.1523727 (2005).
48. Liang, Y., Poor, H. V. & Shamai, S. Secure communication over fading channels. *IEEE Trans. Inf. Theory* **54**, 2470–2492 (2008).
49. Mukherjee, A. & Swindlehurst, A. L. Robust beamforming for security in mimo wiretap channels with imperfect csi. *IEEE Trans. Signal Process.* **59**, 351–361. https://doi.org/10.1109/TSP.2010.2078810 (2011).
50. Shlezinger, N., Zahavi, D., Murin, Y. & Dabora, R. The secrecy capacity of gaussian mimo channels with finite memory. *IEEE Trans. Inf. Theory* **63**, 1874–1897. https://doi.org/10.1109/TIT.2017.2648742 (2017).
51. Yang, Q., Wang, H.-M., Zhang, Y. & Han, Z. Physical layer security in mimo backscatter wireless systems. *IEEE Trans. Wirel. Commun.* **15**, 7547–7560. https://doi.org/10.1109/TWC.2016.2604800 (2016).
52. Rothe, S. *et al.* Physical layer security in multimode fiber optical networks. *Sci. Rep.* **10**, 1–11 (2020).
53. Zhuang, Y. & Lampe, L. Physical layer security in mimo power line communication networks. In *18th IEEE International Symposium on Power Line Communications and Its Applications*, 272–277. https://doi.org/10.1109/ISPLC.2014.6812346 (2014).
54. Camponogara, A., Poor, H. V. & Ribeiro, M. V. Plc systems under the presence of a malicious wireless communication device: Physical layer security analyses. *IEEE Syst. J.* **14**, 4901–4910. https://doi.org/10.1109/JSYST.2020.2969044 (2020).
55. Camponogara, A., Poor, H. V. & Ribeiro, M. V. Physical layer security of in-home plc systems: Analysis based on a measurement campaign. *IEEE Syst. J.* **15**, 617–628. https://doi.org/10.1109/JSYST.2020.2999487 (2021).
56. El Shafie, A., Marzban, M. F., Chabaan, R. & Al-Dhahir, N. An artificial-noise-aided secure scheme for hybrid parallel plc/wireless ofdm systems. In *2018 IEEE International Conference on Communications (ICC)*, 1–6. https://doi.org/10.1109/ICC.2018.8422901 (2018).
57. Salem, A., Rabie, K. M., Hamdi, K. A., Alsusa, E. & Tonello, A. M. Physical layer security of cooperative relaying power-line communication systems. In *2016 International Symposium on Power Line Communications and its Applications (ISPLC)*, 185–189. https://doi.org/10.1109/ISPLC.2016.7476261 (2016).

58. Zhang, J., Liu, X. & Xu, D. Physical layer security based on full-duplex under the impact of channel convergence. In *2021 IEEE 21st International Conference on Communication Technology (ICCT)*, 259–262. https://doi.org/10.1109/ICCT52962.2021.9657986 (2021).
59. Prasad, G., Taghizadeh, O., Lampe, L. & Mathar, R. Securing mimo power line communications with full-duplex jamming receivers. In *2019 IEEE International Symposium on Power Line Communications and its Applications (ISPLC)*, 1–6. https://doi.org/10.1109/ISPLC.2019.8693263 (2019).
60. Camponogara, A., Souza, R. D. & Ribeiro, M. V. The effective secrecy throughput of a broadband power line communication system under the presence of colluding wireless eavesdroppers. *IEEE Access* **10**, 85019–85029. https://doi.org/10.1109/ACCESS.2022.3197528 (2022).
61. Salem, A., Hamdi, K. A. & Alsusa, E. Physical layer security over correlated log-normal cooperative power line communication channels. *IEEE Access* **5**, 13909–13921. https://doi.org/10.1109/ACCESS.2017.2729784 (2017).
62. Mohan, V., Mathur, A., Aishwarya, V. & Bhargav, S. Secrecy analysis of plc system with channel gain and impulsive noise. In *2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall)*, 1–6. https://doi.org/10.1109/VTCFall.2019.8890986 (2019).
63. Dong, L., Han, Z., Petropulu, A. P. & Poor, H. V. Improving wireless physical layer security via cooperating relays. *IEEE Trans. Signal Process.* **58**, 1875–1888. https://doi.org/10.1109/TSP.2009.2038412 (2010).
64. Zhang, J. & Gursoy, M. C. Collaborative relay beamforming for secure broadcasting. In *2010 IEEE Wireless Communication and Networking Conference*, 1–6. https://doi.org/10.1109/WCNC.2010.5506452 (2010).
65. Zhang, J. & Gursoy, M. C. Relay beamforming strategies for physical-layer security. In *2010 44th Annual Conference on Information Sciences and Systems (CISS)*, 1–6. https://doi.org/10.1109/CISS.2010.5464970 (2010).
66. Vilela, J. P., Bloch, M., Barros, J. & McLaughlin, S. W. Friendly jamming for wireless secrecy. In *2010 IEEE International Conference on Communications*, 1–6. https://doi.org/10.1109/ICC.2010.5502606 (2010).
67. Krikidis, I., Thompson, J. S. & Mclaughlin, S. Relay selection for secure cooperative networks with jamming. *IEEE Trans. Wirel. Commun.* **8**, 5003–5011. https://doi.org/10.1109/TWC.2009.090323 (2009).
68. Zheng, Gan, Choo, Li-Chia. & Wong, Kai-Kit. Optimal cooperative jamming to enhance physical layer security using relays. *IEEE Trans. Signal Process.* **59**(3), 1317–1322. https://doi.org/10.1109/TSP.2010.2092774 (2011).
69. Hamamreh, J. M., Abewa, M. & Lemayian, J. P. New non-orthogonal transmission schemes for achieving highly efficient, reliable, and secure multi-user communications. *RS Open J. Innov. Commun. Technol.* **1** (2020). https://rs-ojict.pubpub.org/pub/tphonik9.
70. Zia, M. F. & Hamamreh, J. M. An advanced non-orthogonal multiple access security technique for future wireless communication networks. *RS Open J. Innov. Commun. Technol.***1** (2020). https://rs-ojict.pubpub.org/pub/s99ykm90.
71. Pagani, P. & Schwager, A. A statistical model of the in-home mimo plc channel based on european field measurements. *IEEE J. Sel. Areas Commun.* **34**, 2033–2044. https://doi.org/10.1109/JSAC.2016.2566158 (2016).
72. Zimmermann, M. & Dostert, K. Analysis and modeling of impulsive noise in broad-band powerline communications. *IEEE Trans. Electromagn. Compat.* **44**, 249–258. https://doi.org/10.1109/15.990732 (2002).
73. Tan, B. & Thompson, J. Capacity evaluation with channel estimation error for the decode-and-forward relay plc networks. In *2011 19th European Signal Processing Conference*, 834–838 (IEEE, 2011).
74. Geraci, G., Singh, S., Andrews, J. G., Yuan, J. & Collings, I. B. Secrecy rates in broadcast channels with confidential messages and external eavesdroppers. *IEEE Trans. Wirel. Commun.* **13**, 2931–2943. https://doi.org/10.1109/TWC.2014.041014.131101 (2014).
75. Horn, R. A. & Johnson, C. R. *Matrix Analysis* (Cambridge University Press, 2012).
76. Gharavol, E. A. & Larsson, E. G. The sign-definiteness lemma and its applications to robust transceiver optimization for multiuser mimo systems. *IEEE Trans. Signal Process.* **61**, 238–252. https://doi.org/10.1109/TSP.2012.2222379 (2013).

Author contributions

J.C. and Z.K. conceived study conception and design. J.C. and Z.K. conceived the experiments. J.C. and Z.K. and L.D. made draft manuscript preparation. J.C. and Z.K. conducted the experiments. L.D., T.H. and S.Y. analysed the results. All authors reviewed the manuscript.

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to L.D.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.