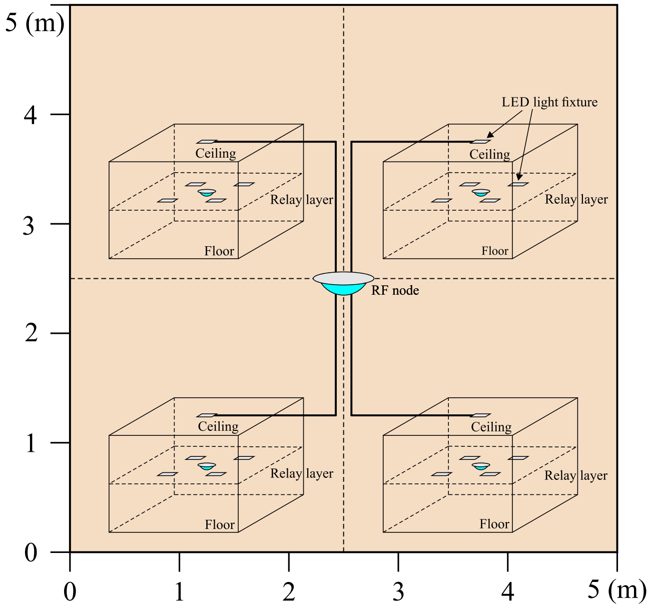
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

# Joint Beamforming Design and Power Minimization for Friendly Jamming Relaying Hybrid RF/VLC Systems

Volume 11, Number 2, April 2019

Jaber Al-Khori
Galymzhan Nauryzbayev, *Member, IEEE*
Mohamed M. Abdallah, *Senior Member, IEEE*
Mounir Hamdi, *Fellow, IEEE*



DOI: 10.1109/JPHOT.2019.2905896

# Joint Beamforming Design and Power Minimization for Friendly Jamming Relaying Hybrid RF/VLC Systems

**Jaber Al-Khori**,[1] **Galymzhan Nauryzbayev**,[2] ***Member, IEEE***,
**Mohamed M. Abdallah**,[1] ***Senior Member, IEEE***,
**and Mounir Hamdi**,[1] ***Fellow, IEEE***

[1]Division of Information and Computing Technology, College of Science and Engineering,
Hamad Bin Khalifa University, Qatar Foundation, Doha, P.O. Box 34110, Qatar
[2]Department of Electrical and Computer Engineering, School of Engineering, Nazarbayev
University, Astana 010000, Kazakhstan

*DOI:10.1109/JPHOT.2019.2905896*

Manuscript received December 29, 2018; revised March 11, 2019; accepted March 14, 2019. Date of publication March 19, 2019; date of current version April 2, 2019. The publication of this article was funded by the Qatar National Library. Corresponding author: Jaber Al-Khori (e-mail: jalkhori@mail.hbku.edu.qa).

**Abstract:** In this paper, we study physical layer security (PLS) aspects of a hybrid radio frequency (RF)/visible light communication (VLC) system with multiple decode-and-forward relaying nodes equipped with friendly jamming capabilities. We first propose a novel joint relay–jammer selection algorithm to enhance the secrecy performance of the network. Next, we obtain beamforming vectors and the minimal power values, which satisfy the required secrecy threshold. Our simulation results show that the proposed hybrid RF/VLC scheme obtains higher secrecy capacity compared to the standalone VLC and RF technologies. Finally, we proved the proposed technique to be an eavesdropping-resilient PLS solution.

**Index Terms:** Beamforming (BF), optimization, physical layer security (PLS), radio frequency (RF), relaying, secrecy, visible light communication (VLC).

## 1. Introduction

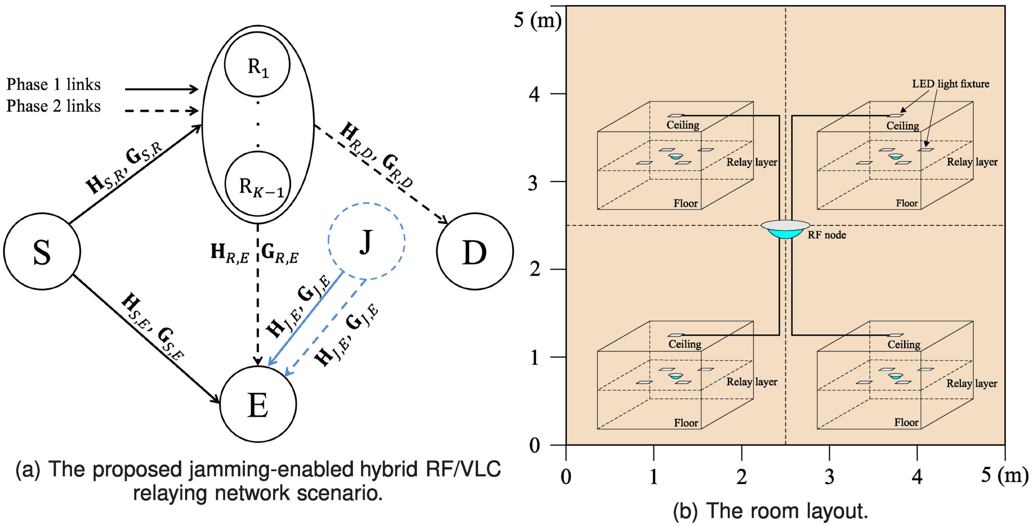
Due to the unprecedented expansion of wireless traffic volumes in the radio frequency (RF) spectrum (for instance, Internet of Things (IoT) is one of the reasons of such spectrum contingency [1]), industrial and academic players have recently proposed to exploit visible light communication (VLC) technology. One of the main advantages of the VLC is that it can be simultaneously used for illumination and communication purposes in a wide unregulated spectrum range (from 430 THz to 790 THz) [2]–[7]. This consequently implies the reduction of deployment and operational costs. Moreover, mutual electromagnetic immunity of the RF and VLC networks can be considered as another benefit of the VLC technology. As with any technology, VLC has its own limitation such as communication unreliability when its line-of-sight (LOS) nature restricts the signal propagation [8]. And this drawback can be properly addressed by introducing a comprehensive hybrid RF/VLC system combining both RF and VLC technologies [9]–[12]. In [13], the authors demonstrated that in the RF congested network, VLC can support its RF counterpart by processing the RF traffic in addition to its own data volume. Moreover, the advantage of the hybrid architecture in terms of energy efficiency (EE) over the standalone RF system was shown in [14]. Additionally, an indoor hybrid RF/VLC communication system when the VLC technology was used to complement an RF communication was considered in [15]; moreover, for the similar system model, a handover technique was proposed in [16] to improve the system throughput. Furthermore, it was shown that better throughput and delay results can be achieved in comparison to the standalone VLC or RF system.

### 1.1 Background

Using relays can significantly improve the network coverage for both RF and VLC systems [17]–[29]. In [17], the authors studied RF relaying networks and investigated the impact of the relay location on the capacity of cell-edge users. Moreover, the outage probability (OP) of the underlay cognitive radio (CR) relaying network with decode-and-forward (DF) relaying was studied in [18]–[21]. On the other hand, the authors in [23] evaluated the spectral efficiency and the ergodic capacity of the amplify-and-forward (AF) relaying network. Furthermore, the authors in [24] considered the wireless powered CR relaying network and corresponding bit-error rate (BER) metric was evaluated. On the other hand, the full-duplex VLC relaying was studied in [25] where the BER results disclosed the advantage of using relays compared to the systems with direct end-to-end communication. In [26], [27], it was shown that the ergodic capacity and outage performance metrics can be improved with relay placement in wireless powered AF-based relaying networks. On the other hand, energy harvesting (EH) was proposed in [28] to enhance the network coverage in hybrid RF/VLC DF relaying systems. [29] also studied a hybrid RF/VLC network with the EH-enabled relay with imposed latency constraints.

Wireless broadcast nature compromises information confidentiality and makes it more vulnerable to eavesdropping activities. Securing such wireless transmission can be maintained by a means of upper layer security techniques (e.g., data encryption, etc.) which require significant computational and processing power [30], [31]. Another promising approach in securing wireless communication is physical layer security (PLS) which has recently attained sufficient research interest as a viable solution able to prevent various eavesdropping and jamming attacks [32]–[37]. For instance, [37] proposed a novel wireless relaying system with cooperative jamming (CJ) to enhance the network performance. Furthermore, in [38], the authors practically applied the CJ to the RF relaying system and derived a suboptimal solution in its closed form to filter the jamming signal out at the user of interest. Another work on PLS [39] proposed an optimal relay selection scheme in cooperative DF- and AF-based RF relaying systems to prevent unauthorized access; moreover, the results demonstrated that the proposed approach provides better performance than the conventional relay selection scheme. In [40], the authors designed a destination-assisted CJ method aiming to maximize the secrecy rate in the wireless RF networks. At the same time, the authors in [41] exploited an access point cooperation to enhance the achievable ergodic secrecy capacity in multiuser VLC networks. Additionally, the lower tight bounds on the outage probability and ergodic secrecy capacity were derived. Beamforming (BF) techniques in VLC networks were studied in [42], [43] where the authors investigated the maximum achievable data rate region and secrecy outage probability, respectively. Finally, using jamming concept to secure the VLC network was studied in [44], where the authors derived a closed-form expression of the secrecy rate. In contrast to the standalone RF and VLC systems, it was shown in [14]–[16], [45], [46] that the hybrid RF/VLC DF relaying network improves the system performance in terms of EE, throughput, secrecy capacity (SC), etc. Moreover, joint relay-jammer selection has a potential to enhance the secrecy of the communication but, to the best of our knowledge, it has not been investigated in the hybrid RF/VLC relaying networks.

To fill this research gap, we investigate an indoor hybrid RF/VLC system with multiple DF relays with jamming capabilities. We first propose a novel joint relay-jammer selection scheme which chooses the relay node based on the minimum outage probability and then selects the jamming node with respect to the best signal-to-noise ratio (SNR) at the eavesdropper location. Next, we propose beamforming design for both RF and VLC subsystems and then exploit it in the formulation of the power minimization problem. Moreover, we evaluate the achievable secrecy capacity and compare it with different benchmark technologies to validate the supremacy of the proposed technique. Finally, we showed the advantage of use of the jammer as an eavesdropping-resilient solution.


Phase 1 links
Phase 2 links
$R_1$
$R_{K-1}$
S
J
D
E
$\mathbf{H}_{S,R}, \mathbf{G}_{S,R}$
$\mathbf{H}_{R,D}, \mathbf{G}_{R,D}$
$\mathbf{H}_{R,E}$ $\mathbf{G}_{R,E}$
$\mathbf{H}_{S,E}, \mathbf{G}_{S,E}$
$\mathbf{H}_{J,E}, \mathbf{G}_{J,E}$
$\mathbf{H}_{J,E}, \mathbf{G}_{J,E}$
5 (m)
4
3
2
1
0
0
1
2
3
4
5 (m)
LED light fixture
Ceiling
Relay layer
Floor
RF node

(a) The proposed jamming-enabled hybrid RF/VLC relaying network scenario.

(b) The room layout.

Fig. 1. An indoor hybrid RF/VLC DL relaying network scenario with multiple jamming-enabled relays.

The remainder of the paper is organized as follows. Section 2 describes the system model of the indoor downlink (DL) hybrid RF/VLC relaying network scenario with multiple jamming-enabled relays. Section 3 demonstrate the design of beamforming vectors for the RF and VLC subsystems while Section 4 defines the secrecy capacity as the PLS performance metric. The power minimization problem is formulated in Section 5. Section 6 presents and discusses the numerical results. Finally, Section 7 concludes the paper.

*Notations:* **A** and **a** denote the matrices and vectors, respectively. $(\cdot)^H$ and $(\cdot)^T$ stand for the conjugate transpose and the matrix transpose, accordingly. $\mathbb{E}$ and $\mathbb{C}$ denote the expected value and complex matrix, respectively, while $\forall$ and $\sum$ mean "for all" and "summation", respectively.

## 2. System Model

The system model given in Fig. 1 represents an indoor hybrid RF/VLC DL relaying network scenario consisting of the source ($S$), eavesdropper ($E$), multiple $K$ DF-based relays ($R_k$, $k \in K$) and destination ($D$) node. We assume there is no direct $S - D$ link between, and therefore the data flow has to be communicated via a selected $R$ within time period $T$ equally divided into two transmission time slots (TSs). The $S \rightarrow R$ communication takes place within TS 1 while the $R \rightarrow D$ transmission is realized over TS 2, where the coordinates of $D$ are given by $(x_D, y_D, z_D)$. Moreover, we assume that $E$ (with the coordinates $(x_E, y_E, z_E)$) has an ability to intercept the signals in both phases (see Fig. 1a). Moreover, we assume that a jamming node ($J$) will be selected from the pool of relaying nodes to secure the communication. Next, the RF and VLC subsystems of the considered hybrid RF/VLC system will be described, with one data stream per subsystem, i.e., $l^{[\mathrm{rf}]} = l^{[\mathrm{vlc}]} = 1$.

### 2.1 The RF Subsystem

In TS 1, $S$ transmits the message $x$ to $R$ which decodes and forwards it to $D$ in TS 2. At the same time, $J$ transmits the jamming signal during both TSs. Therefore, the received signal at the user of interest[1] can be expressed as

$$\mathbf{y}_j(t) = \sqrt{\frac{P_i}{d_{i,j}^{[\mathrm{rf}]\tau}}}\mathbf{H}_{i,j}\mathbf{v}_i x(t) + \mathbf{n}_j(t), j \in \{R, D\}, i \in \{S, R\}, \qquad (1)$$

[1] Since the legitimate user (relay and destination) has a priori knowledge of the jamming signal, it can be filtered out from the overall received signal, which can be realized in practice only at the price of a small amount of overhead [48], [49].

where $\mathbf{H}_{i,j} \in \mathbb{C}^{M_i \times M_j}$ indicates the channel matrix between transmitter $i$ and receiver $j$, which coefficients are assumed to be drawn from independent and identically distributed (i.i.d.) statistical model following $\mathcal{CN}(0, 1)$ and remain constant during time period $T$ [47]. It is assumed that all entities are deployed with multiple $M$ antennas, i.e., $M = M_i = M_j = M_E$. $d_{i,j}^{[\mathrm{rf}]}$ stands for the distance between transmitter $i$ and receiver $j$, and $\tau$ represents the path loss exponent. $\mathbf{v}_{(\cdot)} \in \mathbb{C}^{M \times 1}$ and $P_{(\cdot)} \leq P_{(\cdot)_{\max}}$ are the BF vector and the transmit power available at a certain node, respectively. $x$ denotes the desired signal, with $\mathbb{E}\{|x|^2\} = 1$. $\mathbf{n}_{(\cdot)}$ denotes the zero-mean additive white Gaussian noise (AWGN) at a certain receiver, with variance $\sigma^2$ (without loss of generality, we can assume $\sigma^2 = \sigma_j^2 = \sigma_E^2$). In the following equations, we omit time indexing for simplicity.

On the other hand, the received signal at the $E$ can be expressed as

$$\mathbf{y}_{i,E}(t) = \sqrt{\frac{P_i}{d_{i,E}^{[\mathrm{rf}]\tau}}}\mathbf{H}_{i,E}\mathbf{v}_i x(t) + \sqrt{\frac{P_J}{d_{J,E}^{[\mathrm{rf}]\tau}}}\mathbf{H}_{J,E}\mathbf{v}_J q(t) + \mathbf{n}_E(t), i \in \{S, R\}, \tag{2}$$

where $\mathbf{H}_{i,E} \in \mathbb{C}^{M_i \times M_E}$ indicates the channel matrix between transmitter $i$ and receiver $E$ and $\mathbf{H}_{J,E} \in \mathbb{C}^{M_J \times M_E}$ indicates the channel matrix between $J$ and $E$. $d_{i,E}^{[\mathrm{rf}]}$ and $d_{J,E}^{[\mathrm{rf}]}$ stand for the distance between transmitter $i$ and receiver $E$, and stand for the distance between $J$ and $E$, respectively. $q$ denotes the jamming signal, with $\mathbb{E}\{|q|^2\} = 1$.

### 2.2 The VLC Subsystem

This section describes the VLC subsystem consisting of $S$ and $R$ with a number of light emitting diodes (LEDs). The optical signal can be transmitted through a channel $\mathbf{G}$ consisting of channel coefficients modeled as [6], [7] $g = \frac{A_{PD}(m+1)}{2\pi d^2} \cos^m \phi T_s(\psi) G(\psi) \cos \psi$, if $0 \leq \psi \leq \psi_c$; otherwise, it equals to 0. $A_{PD}$ and $m$ denote the area of the photo-detector (PD) and the order of Lambertian emission (with a half irradiance semi-angle of $\phi_{\frac{1}{2}}$), respectively. $d$ stands for the LOS distance between LED and PD. $\psi$ and $\phi$ indicate the angle of incidence and the angle of irradiance measured from the receiver axis, respectively. $\psi_{FoV}$ is the receiver field-of-view (FoV). $T_s(\psi)$ and $G(\psi)$ denote the signal transmission of the filter and the concentrator gain, respectively.

The relay node detects and forwards the desired signal to the destination, and, therefore, the received signal at the user of interest[2] can be written as

$$\mathbf{r}_j = \rho_j \kappa_i N_i \mathbf{G}_{i,j} \mathbf{w}_i s + \mathbf{z}_j, j \in \{R, D\}, i \in \{S, R\}, \tag{3}$$

Without loss of generality, we assume that the nodes can be characterized by the same PD and LED features, i.e., PD responsivity, $\rho = \rho_E = \rho_j$, and LED scaling factors, $\kappa = \kappa_i = \kappa_J$, respectively. $N_i$ indicates the number of LEDs per light fixture at transmitter $i$. $\mathbf{w}_i$ and $\mathbf{G}_{i,j}$ represent the BF vector deployed at transmitter $i$ and the channel matrix between transmitter $i$ and receiver $j$. $s$ denotes the desired signal. $\mathbf{z}_{(\cdot)}$ stands for the real-valued zero-mean AWGN term, with variance $\epsilon^2$ ($\epsilon^2 = \epsilon_j^2 = \epsilon_E^2$).

The received signal at the $E$ can be expressed as

$$\mathbf{r}_{i,E} = \rho_E \kappa_i N_i \mathbf{G}_{i,E} \mathbf{w}_i s + \rho_E \kappa_J N_J \mathbf{G}_{J,E} \mathbf{w}_J c + \mathbf{z}_E, i \in \{S, R\}, \tag{4}$$

where $N_J$ indicates the number of LEDs per light fixture at the $J$. $\mathbf{w}_J$ represents the BF vector deployed at $J$. $\mathbf{G}_{i,E}$ and $\mathbf{G}_{J,E}$ represent the channel matrix between transmitter $i$ and $E$, and the channel matrix between $J$ and $E$, respectively. $c$ denotes the jamming signal.

[2] In VLC systems, it is feasible to filter out the jamming signal from the desired signal by placing it into a subspace orthogonal to the channel [50], [51]

### *2.3 Joint Relay-Jammer Selection Scheme*

Following (1) and (3) and considering the availability of multiple relays, we can express the corresponding RF and VLC SNR values at node $j \in \{R_k, D\}$ as

$$\gamma_{i,j} = \frac{P_i \sum_{m=1}^{M} |\mathbf{H}_{i,j}(m)\mathbf{v}_i|^2}{d_{i,j}^{[\mathrm{rf}]\tau}\sigma_j^2}, \; i \in \{S, R_k\}, \tag{5}$$

$$\zeta_{i,j} = \frac{\left(\rho_j N_i \kappa_i \sum_{f=1}^{F} (\mathbf{G}_{i,j}(f)^T \mathbf{w}_i)\right)^2 \bar{P}_i}{\epsilon_j^2}, \tag{6}$$

where $\mathbf{H}_{i,j}(m)$ and $\mathbf{G}_{i,j}(f)$ denote the $m$th row of $\mathbf{H}_{i,j}$ and the $f$th row of $\mathbf{G}_{i,j}$, respectively.[3] $\mathbf{v}_i$ and $\mathbf{w}_i$ are the BF vectors associated with broadcast omni-directional transmission when no preference in direction exists and they satisfy unity power constraint, i.e., $\text{trace}\left(\mathbf{v}_i\mathbf{v}_i^H\right) = \text{trace}\left(\mathbf{w}_i\mathbf{w}_i^T\right) = 1$.

A certain relay will be selected for data transmission based on the outage performance metric as follows: since the system model comprises two subsystems, i.e., RF and VLC, the overall capacity achieved by a relay $k$ can be expressed as $C_k = \mathcal{R}_k + \mathcal{I}_k$, where $\mathcal{R}_k$ and $\mathcal{I}_k$ are the end-to-end capacities for the RF and VLC subsystems which can be calculated as

$$\mathcal{R}_k = \frac{1}{2}\log_2\left(1 + \min\left(\gamma_{S,R_k}, \gamma_{R_k,D}\right)\right), \tag{7}$$

$$\mathcal{I}_k = \frac{1}{2}\log_2\left(1 + \min\left(\frac{2\zeta_{S,R_k}}{\pi e}, \frac{2\zeta_{R_k,D}}{\pi e}\right)\right). \tag{8}$$

The outage event occurs when a certain rate $\Delta_{\text{th}}$ is not supported by the system and can be written as

$$\begin{aligned}
P_{\text{out},k} &= \Pr\left(C_k < \Delta_{\text{th}}\right), \\
&= \Pr\left(\frac{1}{2}\log_2\left(1 + \min\left(\gamma_{S,R_k}, \gamma_{R_k,D}\right)\right) + \frac{1}{2}\log_2\left(1 + \min\left(\frac{2\zeta_{S,R_k}}{\pi e}, \frac{2\zeta_{R_k,D}}{\pi e}\right)\right) < \Delta_{\text{th}}\right) \\
&= \Pr\left(\min\left(\gamma_{S,R_k}, \gamma_{R_k,D}\right) + \min\left(\frac{2\zeta_{S,R_k}}{\pi e}, \frac{2\zeta_{R_k,D}}{\pi e}\right)\right. \\
&\quad \left. + \min\left(\gamma_{S,R_k}, \gamma_{R_k,D}\right)\min\left(\frac{2\zeta_{S,R_k}}{\pi e}, \frac{2\zeta_{R_k,D}}{\pi e}\right) < \nu_{\text{th}}\right),
\end{aligned} \tag{9}$$

where $\nu_{\text{th}} = 2^{2\Delta_{\text{th}}} - 1$ is the corresponding SNR threshold. Then, the relay with the lowest outage will be chosen for data transmission as

$$k^* = \arg\min \mathbf{P}_{\text{out}} \rightarrow R, \tag{10}$$

where $\mathbf{P}_{\text{out}} = [P_{\text{out},1}, \ldots, P_{\text{out},K}]$.

After choosing the relay for data transmission, we have a set of remaining relays among which the jammer will be selected to secure the communication session against $E$ as

$$\underset{\forall k \neq k^*}{\arg\max}\, \Gamma(\alpha) \rightarrow J, \tag{11}$$

where $\Gamma(\alpha) = [\Gamma(\alpha, 1), \ldots, \Gamma(\alpha, K)]$ and $\Gamma(\alpha, k) = \alpha\zeta_{R_k,E} + (1-\alpha)\gamma_{R_k,E}$. $0 \leq \alpha \leq 1$ represents a weighting factor defining which model, RF or VLC, is set with a higher priority in jamming.[4] This implies that the relaying node with the maximum sum of the weighted SNRs observed by $E$ is

[3] To effectively turn the available channel gains to advantage, we apply multiple-input multiple-output (MIMO) maximal ratio combining (MRC) technique for both VLC and RF subsystems. Therefore, the effective received signal can be expressed as a sum of the signal replicas observed from all receive antenna branches [52].

[4] In the case when no privilege is given to any subsystem, we set $\alpha = 0.5$.

**Algorithm 1:** The Joint Relay-Jammer Selection.

```
Require:
 1: inputs $K$, $\mathbf{H}_{i,j}$, $\mathbf{G}_{i,j}$, $\mathbf{H}_{R_k,E}$, $\mathbf{G}_{R_k,E}$, $P_{i\,\max}$, $\bar{P}_{i\,\max}$, $\Delta_{\text{th}}$, $\alpha$, $\rho_j$, $\rho_E$, $\kappa_i$, $N_i$, $\sigma^2$, $\epsilon^2$, $d_{i,j}^{[\text{RF}]}$, $d_{i,E}^{[\text{RF}]}$,
      $\forall i \in \{S, R_k\}$, $j \in \{R_k, D\}$, $k \in K$
Ensure:
 2: This part is dedicated for the relay selection
 3: generate $\mathbf{v}_i$ and $\mathbf{w}_i$ satisfying trace $(\mathbf{v}_i\mathbf{v}_i^H) = $ trace $(\mathbf{w}_i\mathbf{w}_i^T) = 1$
 4: for $k$ do
 5:     calculate the SNR values according to (5) and (6) using given inputs
 6:     then evaluate the capacity of the RF and VLC subsystems according to (7) and (8)
 7:     calculate the outage probability for each relay using (9)
 8:     return $P_{\text{out},k}$
 9: end for
10: find the minimum outage among $K$ relays, i.e., arg min $\mathbf{P}_{\text{out}}$
11: return $k^*$ to select the relay for data transmission
12: This part is dedicated for the jammer selection
13: for $k$ do
14:     calculate the SNR values according to (12) and (13) using given inputs
15:     then evaluate $\Gamma(\alpha, k) = \alpha\zeta_{R_k,E} + (1-\alpha)\,\gamma_{R_k,E}$
16:     return $\Gamma(\alpha, k)$
17: end for
18: find the maximum for $\Gamma(\alpha)$ according to (11)
19: return $k'$ to select the jammer
20: if $k' == k^*$ then
21:     remove $k'$ from the selection process
22:     repeat Steps 13–19
23: else
24:     return $R \leftarrow R_{k^*}$ and $J \leftarrow R_{k'}$.
25: end if
```

chosen to be $J$ while the rest of relays remain idle. The corresponding RF- and VLC-based SNR values $\gamma_{R_k,E}$ and $\zeta_{R_k,E}$ can be expressed as

$$\gamma_{R_k,E} = \frac{P_{R_k}\sum_{m=1}^{M}|\mathbf{H}_{R_k,E}(m)\mathbf{v}_{R_k}|^2}{d_{R_k,E}^{[\text{rf}]\tau}\sigma_E^2},\ k \neq k^*, \tag{12}$$

$$\zeta_{R_k,E} = \frac{\left(\rho_E N_{R_k}\kappa_{R_k}\sum_{f=1}^{F}(\mathbf{G}_{R_k,E}(f)^T\mathbf{w}_{R_k})\right)^2 \bar{P}_{R_k}}{\epsilon_E^2},\ k \neq k^*, \tag{13}$$

where $F$ denotes the number of deployed light fixtures.

The proposed joint relay-jammer selection scheme is presented in Algorithm 1.

## 3. Beamforming Design

### 3.1 RF Beamforming

Since the information needs to be communicated via a selected $R$ over two TSs, as a result, we have to get two sets of the BF vectors.

The optimization that maximizes the capacity of the $S \to R$ and $R \to D$ links while securing the communication from $E$ can be given as

$$\underset{\mathbf{v}_i}{\text{maximize}} \sum_{m=1}^{M} \mathbf{H}_{i,j}(m)\mathbf{v}_i \tag{14a}$$

$$\text{subject to } \mathbf{v}_i^H \mathbf{v}_i \le 1, \tag{14b}$$

where $i \in \{S, R\}$ and $j \in \{R, D\}$. The objective in (14a) is a linear function and the provided constraint is convex. Therefore, the capacity maximization is a convex problem that can be solved using Lagrangian duality [53]. Hence, the objective and constraint functions can be combined as

$$L_{i,j} = -\sum_{m=1}^{M} \mathbf{H}_{i,j}(m)\mathbf{v}_i + \nu_{i,j}(\mathbf{v}_i^H \mathbf{v}_i - 1), \tag{15}$$

where $\nu_{i,j}$ is the Lagrangian multiplier. By applying Karush-Kuhn-Tucker (KKT) conditions [53], we obtain the optimum RF subsystem BF vectors as the following,

$$\mathbf{v}_i = \frac{\sum_{m=1}^{M} \mathbf{H}_{i,j}^H(m)}{2\nu_{i,j}}, \tag{16}$$

By using the KKT conditions and Lagrangian duality, the optimum values of Lagrangian multipliers can be obtained as

$$\nu_{i,j} = \sqrt{\frac{\sum_{m=1}^{M} \mathbf{H}_{i,j}(m) \sum_{m=1}^{M} \mathbf{H}_{i,j}^H(m)}{4}}. \tag{17}$$

At the same time, the jammer aims to disrupt the signal reception at $E$ as follows

$$\underset{\mathbf{v}_J}{\text{maximize}} \sum_{m=1}^{M} \mathbf{H}_{J,E}(m)\mathbf{v}_J \tag{18a}$$

$$\text{subject to } \sum_{m=1}^{M} \mathbf{H}_{J,j}(m)\mathbf{v}_J = 0 \tag{18b}$$

$$\mathbf{v}_J^H \mathbf{v}_J \le 1, \tag{18c}$$

where $j \in \{R, D\}$. (18a) is linear and the constraints given by (18b) and (18c) are convex. Similar to the problem defined in (14a) and (14b), this optimization problem is convex which can be solved applying Lagrangian duality [53]. The objective function and constraints can be written as

$$L_J = -\sum_{m=1}^{M} \mathbf{H}_{J,E}(m)\mathbf{v}_J + \lambda_{1J}(\mathbf{v}_J^H \mathbf{v}_J - 1) + \lambda_{2J} \sum_{m=1}^{M} \mathbf{H}_{J,R}(m)\mathbf{v}_J, \tag{19}$$

where $\lambda_{1J}$ and $\lambda_{2J}$ are the Lagrangian multipliers. By using the KKT conditions [53], the optimum RF BF vectors can be obtained as

$$\mathbf{v}_J = \frac{\sum_{m=1}^{M} \mathbf{H}_{J,E}^H(m) - \lambda_{2J} \sum_{m=1}^{M} \mathbf{H}_{J,j}^H(m)}{2\lambda_{1J}}. \tag{20}$$

Hence, the optimum values of Lagrangian multipliers can be found as

$$\lambda_{1J} = \sqrt{\frac{\beta_1 - \beta_2 - \beta_3 + \beta_4}{4}}, \tag{21}$$

where $\beta_1 = \sum_{m=1}^{M} \mathbf{H}_{J,E}(m) \sum_{m=1}^{M} \mathbf{H}_{J,E}^{H}(m)$, $\beta_2 = \lambda_{2J} \sum_{m=1}^{M} \mathbf{H}_{J,j}(m) \sum_{m=1}^{M} \mathbf{H}_{J,E}^{H}(m)$, $\beta_3 = \lambda_{2J} \sum_{m=1}^{M} \mathbf{H}_{J,E}(m) \sum_{m=1}^{M} \mathbf{H}_{J,j}^{H}(m)$ and $\beta_4 = \lambda_{2J}^{2} \sum_{m=1}^{M} \mathbf{H}_{J,j}(m) \sum_{m=1}^{M} \mathbf{H}_{J,j}^{H}(m)$,

$$\lambda_{2J} = \frac{\sum_{m=1}^{M} \mathbf{H}_{J,j}(m) \sum_{m=1}^{M} \mathbf{H}_{J,E}^{H}(m)}{\sum_{m=1}^{M} \mathbf{H}_{J,j}(m) \sum_{m=1}^{M} \mathbf{H}_{J,j}^{H}(m)}. \tag{22}$$

### 3.2 VLC Beamforming

This section presents the design of two sets of the VLC BF weights to maximize the achievable SC that can be formulated as

$$\underset{\mathbf{w}_i}{\text{maximize}} \sum_{f=1}^{F} \mathbf{G}_{i,j}^{T} \mathbf{w}_i \tag{23a}$$

$$\text{subject to } -\mathbf{1} \leq \mathbf{w}_i \leq \mathbf{1}, \tag{23b}$$

where $i \in \{S, R\}$ and $j \in \{R, D\}$. The problem in (23a) can be solved using a certain linear programming optimizer (e.g., `fmincon` MATLAB built-in function) which will maximize the capacity at the relay and destination nodes. Moreover, the condition (23b) satisfies the unity power constraint. On the other hand, the jammer aims to deteriorate the achievable capacity at $E$ in the way given below as

$$\underset{\mathbf{w}_J}{\text{maximize}} \sum_{f=1}^{F} \mathbf{G}_{J,E}^{T} \mathbf{w}_J \tag{24a}$$

$$\text{subject to} \sum_{f=1}^{F} \mathbf{G}_{J,j}^{T} \mathbf{w}_J = 0 \tag{24b}$$

$$-\mathbf{1} \leq \mathbf{w}_J \leq \mathbf{1}, \tag{24c}$$

where $j \in \{R, D\}$. At the same time, the conditions (24b) and (24c) ensure that the jamming signals will be easily subtracted at the reception of the relay and destination nodes, and the obtained VLC BF vectors will satisfy the unity power constraint, respectively.

## 4. Secrecy Capacity

In this section, we investigate the hybrid RF/VLC DF relaying network scenario and estimate its performance in terms of the secrecy capacity which can be defined as non-negative difference between the channel capacity of $D$ and the capacity achievable by $E$, i.e., $\max(0, \Delta)$ [54], [55].

### 4.1 The RF-Based Secrecy Capacity

The signal-to-interference-plus-noise ratio (SINR) at $E$ can be given as

$$\gamma_{i,E} = \frac{\frac{P_i}{d_{i,E}^{[\mathrm{rf}]\tau}} \sum_{m=1}^{M} |\mathbf{H}_{i,E}(m)\mathbf{v}_i|^2}{\frac{P_J}{d_{J,E}^{[\mathrm{rf}]\tau}} \sum_{m=1}^{M} |\mathbf{H}_{J,E}(m)\mathbf{v}_J|^2 + \sigma_E^2}, \; i \in \{S, R\}. \tag{25}$$

Hence, the instantaneous end-to-end capacity can be written as

$$\mathcal{R} = \frac{1}{2} \log_2 \left(1 + \min\left(\gamma_R, \gamma_D\right)\right). \tag{26}$$

On the other hand, the channel capacity of $E$ during both TSs can be given as

$$\mathcal{R}_{i,E} = \frac{1}{2} \log_2 \left(1 + \gamma_{i,E}\right), i \in \{S, R\}. \tag{27}$$

The corresponding SC values for two TSs can be written as

$$\Delta_j^{[\mathrm{rf}]} = \mathcal{R}_j - \mathcal{R}_{i,E},\ i \in \{S, R\},\ j \in \{R, D\}, \tag{28}$$

where the channel capacity of the $j$th node is given by $\mathcal{R}_j = \frac{1}{2}\log_2\left(1+\gamma_j\right)$.

To capture the worse network scenario, we subtract the maximum channel capacity achievable by $E$ from the effective capacity of $D$. Then, the instantaneous end-to-end SC can be written as

$$\begin{aligned}\Delta^{[\mathrm{rf}]} &= \mathcal{R} - \max\left(\mathcal{R}_{S,E}, \mathcal{R}_{R,E}\right)\\ &= \frac{1}{2}\log_2\left(1+\min\left(\gamma_R, \gamma_D\right)\right) - \frac{1}{2}\log_2\left(1+\max\left(\gamma_{S,E}, \gamma_{R,E}\right)\right)\\ &= \left[\log_2\left(\left(\frac{1+\min\left(\gamma_R, \gamma_D\right)}{1+\max\left(\gamma_{S,E}, \gamma_{R,E}\right)}\right)^{\frac{1}{2}}\right)\right]^+,\end{aligned} \tag{29}$$

where $[y]^+$ indicates $\max\{y, 0\}$. Moreover, to assure the positive SC, the following condition has to be satisfied

$$\min(\gamma_R, \gamma_D) > \max(\gamma_{S,E}, \gamma_{R,E}). \tag{30}$$

### 4.2 The VLC-Based Secrecy Capacity

The received power (RP) levels corresponding to the desired messages during both TSs can be presented as

$$\bar{P}_{RP_j} = \left(\rho_j N_i \kappa_i \sum_{f=1}^{F} \mathbf{G}_{i,j}(f)^T \mathbf{w}_i\right)^2 \bar{P}_i,\ i \in \{S, R\},\ j \in \{R, D\}, \tag{31}$$

where $\bar{P}_i$ is the average consumed electrical power per LED, with $\mathbb{E}\{|s_i|^2\} = \bar{P}_i$ and $\mathbf{G}_{i,j}(f)$ denotes the $f$th row of $\mathbf{G}_{i,j}$. On the other hand, the received power levels at $E$ can be given as

$$\bar{P}_{RP_{i,E}} = \left(\rho_E N_i \kappa_i \sum_{f=1}^{F} \mathbf{G}_{i,E}(f)^T \mathbf{w}_i\right)^2 \bar{P}_i,\ i \in \{S, R, J\}. \tag{32}$$

The SNR related to the received signal of the user of interest given in (3) can be expressed as

$$\zeta_j = \frac{\bar{P}_{RP_j}}{\epsilon_j^2}, j \in \{R, D\}, \tag{33}$$

while the SINR values observed by $E$ can be given as

$$\zeta_{i,E} = \frac{\bar{P}_{RP_{i,E}}}{\bar{P}_{RP_{J,E}} + \epsilon_E^2}, i \in \{S, R\}. \tag{34}$$

The corresponding instantaneous end-to-end capacity can be written as

$$\mathcal{I} = \frac{1}{2}\log_2\left(1+\min\left(\frac{2\zeta_R}{\pi e}, \frac{2\zeta_D}{\pi e}\right)\right). \tag{35}$$

On the other hand, the channel capacity of $E$ can be expressed as

$$\mathcal{I}_{i,E} = \frac{1}{2}\log_2\left(1+\frac{2\zeta_{i,E}}{\pi e}\right), i \in \{S, R\}. \tag{36}$$

Similar to Section 4.1, we define the capacity difference achievable for the $S \rightarrow R$ and $R \rightarrow D$ communication sessions as

$$\Delta_j^{[\mathrm{vlc}]} = \mathcal{I}_j - \mathcal{I}_{i,E},\ i \in \{S, R\},\ j \in \{R, D\}, \tag{37}$$

**Algorithm 2:** The Beamforming Design and Power Minimization.

```
Require:
  inputs $\mathbf{H}_{i,j}, \mathbf{G}_{i,j}, \mathbf{H}_{J\cdot E}, \mathbf{G}_{J,E}, P_{i\,\max}, \bar{P}_{i\,\max}, P_{J\,\max}, \bar{P}_{J\,\max}, \Delta_{\text{th}}, \alpha, N_i\ \forall i \in \{S, R\}, j \in \{R, D\}$
Ensure:
  This part is dedicated for the RF subsystem design
  for $i$ do
    if (14b) is TRUE and using Lagrangian duality and KKT conditions then
      calculate $\mathbf{v}_i$ according to (16)
    end if
    if (18b) && (18c) are TRUE and using Lagrangian duality and KKT conditions then
      calculate $\mathbf{v}_J$ according to (20)
    end if
    return $\mathbf{v}_i$ && $\mathbf{v}_J$
  end for
  This part is dedicated for the VLC subsystem design
  for $i$ do
    if (23b) is TRUE using linear programming optimizer then
      calculate $\mathbf{w}_i$ according to (23a)
    end if
    if (24b) && (24c) are TRUE using linear programming optimizer then
      calculate $\mathbf{w}_J$ according to (24a)
    end if
    return $\mathbf{w}_i$ && $\mathbf{w}_J$
  end for
  These derived vectors $\mathbf{v}_i$, $\mathbf{v}_J$, $\mathbf{w}_i$ and $\mathbf{w}_J$ will be used in the next iteration
  if $\Delta^{[\text{rf}]} + \Delta^{[\text{vlc}]} \geq \Delta_{\text{th}}$ && $P_i \leq P_{i\,\max}$ && $\bar{P}_i \leq \bar{P}_{i\,\max}$ && $P_J \leq P_{J\,\max}$ && $\bar{P}_J \leq \bar{P}_{J\,\max}$ then
    calculate the consumed power according to (40a)
  end if
  return $P_i, \bar{P}_i, P_J, \bar{P}_J, \Delta^{[\text{rf}]}, \Delta^{[\text{vlc}]}$.
```

where the channel capacity of the $j$th node is given by $\mathcal{I}_j = \frac{1}{2}\log_2\left(1 + \zeta_j\right)$.

To consider the worse network scenario, we calculate the capacity difference by subtracting the maximum channel capacity of $E$ from the effective end-to-end channel capacity. Therefore, the VLC-based end-to-end secrecy capacity can be expressed as

$$\begin{aligned}\Delta^{[\text{vlc}]} &= \mathcal{I} - \max\left(\mathcal{I}_{S,E}, \mathcal{I}_{R,E}\right)\\ &= \frac{1}{2}\log_2\left(1 + \min\left(\frac{2\zeta_R}{\pi e}, \frac{2\zeta_D}{\pi e}\right)\right) - \frac{1}{2}\log_2\left(1 + \max\left(\frac{2\zeta_{S,E}}{\pi e}, \frac{2\zeta_{R,E}}{\pi e}\right)\right)\\ &= \left[\log_2\left(\left(\frac{1 + \min\left(\frac{2\zeta_R}{\pi e}, \frac{2\zeta_D}{\pi e}\right)}{1 + \max\left(\frac{2\zeta_{S,E}}{\pi e}, \frac{2\zeta_{R,E}}{\pi e}\right)}\right)^{\frac{1}{2}}\right)\right]^{+}.\end{aligned} \tag{38}$$

Similarly to the RF part, we can ensure the positive secrecy capacity by following

$$\min\left(\zeta_R, \zeta_D\right) > \max\left(\zeta_{S,E}, \zeta_{R,E}\right). \tag{39}$$

## 5. Problem Formulation

This section presents a two-fold minimization problem for the overall consumed power of the considered hybrid RF/VLC DF relaying. We first design the RF- and VLC-based transmit BF vectors (are obtained in Section 3) to enhance the achievable SC while $J$ aims to degrade the capacity of $E$. Since the total achieved secrecy, i.e., $\Delta^{[\text{vlc}]} + \Delta^{[\text{RF}]}$, is restricted by the presence of $E$, our target is to secure the $S \rightarrow R$ and $R \rightarrow D$ communication links in order to prevent the information leakage to the unauthorized user. Then, our goal is to minimize the weighted sum of the consumed electrical power. With this in mind, we formulate this problem as follows

$$\begin{aligned} \underset{\forall P_j, \bar{P}_j, P_J^{[n]}, \bar{P}_J^{[n]}}{\text{minimize}} \; & \alpha N^2 \left[ \bar{P}_S \mathbf{w}_S^T \mathbf{w}_S + \bar{P}_R \mathbf{w}_R^T \mathbf{w}_R + \bar{P}_J^{[1]} \mathbf{w}_J^T \mathbf{w}_J + \bar{P}_J^{[2]} \mathbf{w}_J^T \mathbf{w}_J \right] \\ & + (1-\alpha) \left[ P_S \mathbf{v}_S^H \mathbf{v}_S + P_R \mathbf{v}_R^H \mathbf{v}_R + P_J^{[1]} \mathbf{v}_J^H \mathbf{v}_J + P_J^{[2]} \mathbf{v}_J^H \mathbf{v}_J \right] \end{aligned} \tag{40a}$$

$$\text{subject to } \Delta^{[\text{rf}]} + \Delta^{[\text{vlc}]} \geq \Delta_{\text{th}} \tag{40b}$$

$$P_j \leq P_{j_{\max}} \tag{40c}$$

$$\bar{P}_j \leq \bar{P}_{j_{\max}} \tag{40d}$$

$$P_J^{[n]} \leq P_{J_{\max}} \tag{40e}$$

$$\bar{P}_J^{[n]} \leq \bar{P}_{J_{\max}} \tag{40f}$$

$$\sum_{m=1}^{M} \mathbf{H}_{J,R}(m) \mathbf{v}_J = 0, \tag{40g}$$

$$\sum_{m=1}^{M} \mathbf{H}_{J,D}(m) \mathbf{v}_J = 0 \tag{40h}$$

$$\sum_{f=1}^{F} \mathbf{G}_{J,R}(f) \mathbf{w}_J = 0, \tag{40i}$$

$$\sum_{f=1}^{F} \mathbf{G}_{J,D}(f) \mathbf{w}_J = 0 \tag{40j}$$

$$\mathbf{v}_j^H \mathbf{v}_j \leq 1 \tag{40k}$$

$$\mathbf{v}_J^H \mathbf{v}_J \leq 1 \tag{40l}$$

$$|\mathbf{w}_j| \leq \mathbf{1}, \tag{40m}$$

$$|\mathbf{w}_J| \leq \mathbf{1}, \tag{40n}$$

where $j \in \{S, R\}$, $n \in \{1, 2\}$ and $\alpha$ denotes the weighting factor defining the system priority between the RF and VLC subsystems. The constraint (40b) is to ensure that the system achieves the required SC given by $\Delta_{\text{th}}$ while the constraints specified by (40c)–(40f) are to satisfy the power limitation of the hybrid RF/VLC nodes. The constraints (40g)–(40j) are to guarantee that the jamming signal can be effectively subtracted from the both RF and VLC received signals at the relay and destination nodes, respectively. The constraints (40k)–(40n) to satisfy the power unity of the RF and VLC BF vectors, respectively. Finally, this power minimization problem can be solved by following Algorithm 2.

## 6. Simulation Results

In this section, we present some numerical results on the secrecy capacity and power consumption for the considered indoor hybrid RF/VLC DF network scenario with multiple relays with jamming capabilities. The RF and VLC parameters of the hybrid model are given in Tables 1 and 2, respectively. Moreover, the physical locations of the nodes are presented in Tables 3 and 4. The weighting

TABLE 1
The RF Simulation Parameters

| Parameter | Value |
|---|---|
| Available power per node $j, P_{j_{max}}, j \in \{S, R, J\}$ | $1$ Watt |
| Noise power density per node, $\sigma^2$ | $10^{-3}$ Watt |
| Number of deployed antennas, $M_i$, $i \in \{S, R, D, J, E\}$ | $4$ |
| Path loss exponent ($\tau$) | $2.7$ |

TABLE 2
The VLC Simulation Parameters

| Parameter | Value |
|---|---|
| The order of Lambertian emission, $m$ | $1$ |
| Half irradiance semi-angle, $\phi_{\frac{1}{2}}$ | $60^\circ$ |
| The PD area, $A_{PD}$ | $1$ cm$^2$ |
| Signal transmission of the filter, $T_s(\psi)$ | $1$ |
| The concentrator gain $G(\psi)$ | $1$ |
| The concentrator's field-of-view, $\Psi_c$ | $85^\circ$ |
| Available power per node $j$, $\bar{P}_{j_{max}}$, $j \in \{S, R, J\}$ | $0.3$ Watt |
| Number of light fixtures per node | 4 |
| Number of LEDs per light fixture, $N_i$, $i \in \{S, R, J\}$ | $16$ |
| Noise power density per node, $\epsilon^2$ | $2 \times 10^{-15}$ A$^2$ |
| Scaling factor, $\kappa_j$, $j \in \{S, R, J\}$ | $0.54$ Watt/A |
| The PD responsivity, $\rho_i$, $i \in \{R, D, E\}$ | $0.8$ A/Watt |

TABLE 3
The RF and VLC Nodes Location

| RF nodes | **Location**, $(x, y, z)$, m | VLC nodes | **Location**, $(x, y, z)$, m |
|---|---|---|---|
| $S$ | $(2.5, 2.5, 3)$ | | |
| $R_1$ | $(1.25, 3.75, 2)$ | $S^1$ | $(1.25, 3.75, 3)$ |
| $R_2$ | $(3.75, 3.75, 2)$ | $S^2$ | $(3.75, 3.75, 3)$ |
| $R_3$ | $(3.75, 1.25, 2)$ | $S^3$ | $(3.75, 1.25, 3)$ |
| $R_4$ | $(1.25, 1.25, 2)$ | $S^4$ | $(1.25, 1.25, 3)$ |

factor $\alpha$ in (40a) is set as $\alpha = 0.5$ to provide equal priorities to the both subsystems. Moreover, we set the SC threshold as $\Delta_{\text{th}} = 6$ bits/s/Hz.[5] We assume that the destination node moves within the

[5] Note that we set $\Delta_{\text{th}} = 6$ bits/s/Hz in order to prove the outperformance of the proposed algorithm over the standalone RF or VLC systems based on the selected system parameters presented in Tables 1–2.

TABLE 4
VLC Relays' Location

| VLC nodes | **Location**, $(x, y, z)$, m | VLC nodes | **Location**, $(x, y, z)$, m |
|---|---|---|---|
| $R_1^1$ | $(1.2, 3.8, 2)$ | $R_2^1$ | $(3.7, 3.8, 2)$ |
| $R_1^2$ | $(1.3, 3.8, 2)$ | $R_2^2$ | $(3.8, 3.8, 2)$ |
| $R_1^3$ | $(1.3, 3.7, 2)$ | $R_2^3$ | $(3.8, 3.7, 2)$ |
| $R_1^4$ | $(1.2, 3.7, 2)$ | $R_2^4$ | $(3.7, 3.7, 2)$ |
| $R_3^1$ | $(3.7, 1.3, 2)$ | $R_4^1$ | $(1.2, 1.3, 2)$ |
| $R_3^2$ | $(3.8, 1.3, 2)$ | $R_4^2$ | $(1.3, 1.3, 2)$ |
| $R_3^3$ | $(3.8, 1.2, 2)$ | $R_4^3$ | $(1.3, 1.2, 2)$ |
| $R_3^4$ | $(3.7, 1.2, 2)$ | $R_4^4$ | $(1.2, 1.2, 2)$ |

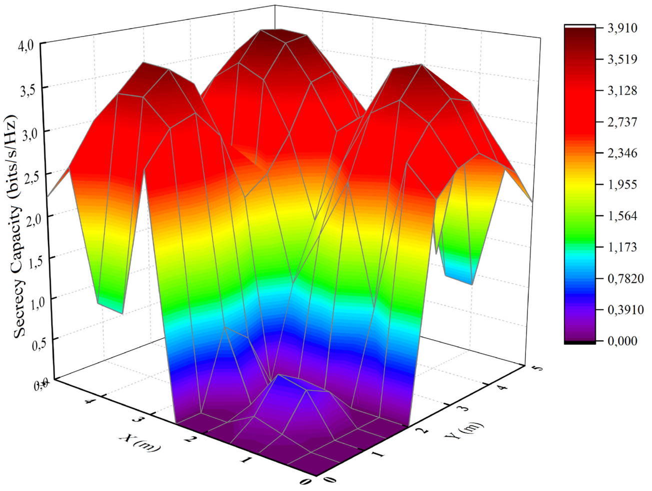


Fig. 2. The SC of the standalone VLC system with respect to the user's location.

room environment with a size of 5 m × 5 m × 3 m (see Fig. 1b) while the location of *E* is kept fixed at (2, 2, 1.5) m.

The results on the achievable SC of the standalone VLC, standalone RF and proposed hybrid RF/VLC systems are depicted in Figs. 2–4. To start with, it is important to highlight that the standalone VLC does not achieve the required secrecy and its maximum achievable SC equals 3.9 bits/s/Hz (see Fig. 2). Another interesting observation is that the VLC experiences severe performance degradation due to the fact that the channels have a deterministic channel model at the location of *E* [47]. Therefore, when *E* and *D* reside close to each other, their channels become more dependent which results in the proximity of the corresponding null spaces. In contrast to the VLC, the standalone RF system achieves maximum 5.3 bits/s/Hz which is still below the required SC threshold as shown in Fig. 3. At the same time, its SC pattern differs from the standalone VLC one and can be characterized by a more smooth surface due to its probabilistic channel behavior. And, therefore, the effect of the correlated channels of *E* and *D* (in small proximity) is less than the one corresponding to the standalone VLC system. Moreover, it can be noticed that the location of *E* deteriorates the achievable SC in the corresponding area and achieves less secrecy compared to the other areas. Next, we consider the secrecy of the proposed hybrid technique presented in Fig. 4 where it can be observed that the required SC of 6 bits/s/Hz is achievable in most of the area

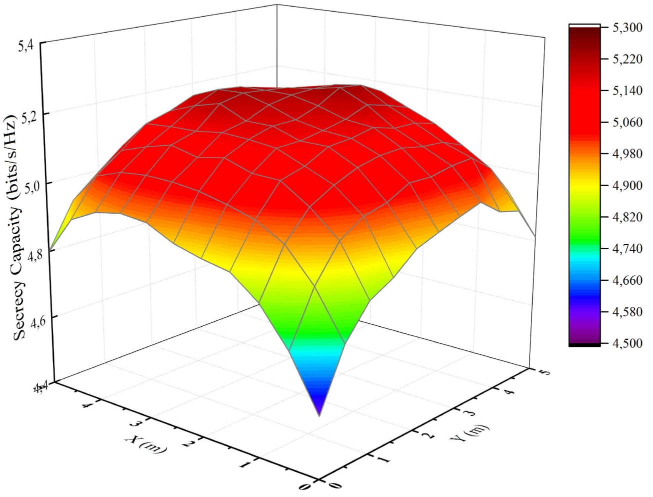


Fig. 3. The SC of the standalone RF system with respect to the user's location.

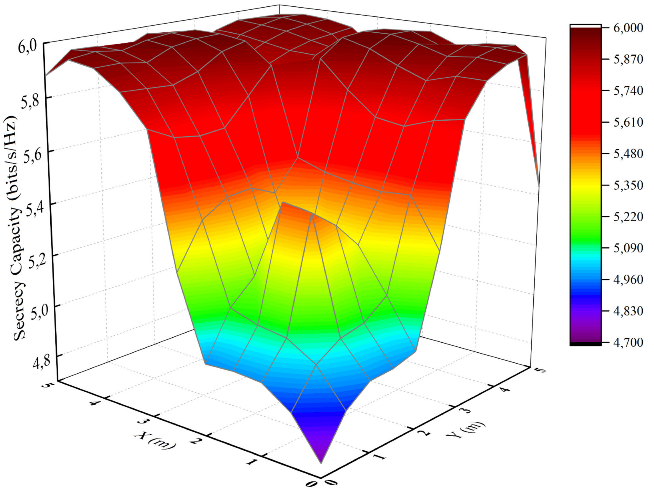


Fig. 4. The SC of the proposed scheme with respect to the user's location.

of the room.[6] Regarding the location of $E$, we can see that the system experiences lower secrecy compared to the other areas and this can be explained by the fact that the VLC subsystem itself has poor performance, as expected. Then, it is obvious that the SC performance of the proposed scheme depends on the RF subsystem due to its relative robustness to the impact of $E$. Since it is obvious that these standalone systems do not achieve the required SC, it can be concluded that it is reasonable to exploit the proposed hybrid RF/VLC system in order to enhance the SC of the network without extra power costs by exploiting existing LED illumination [14].

With this in mind, we plot the results on the power consumption (in dBm) of $S$ and $R$ for the standalone RF and hybrid systems in Figs. 5 and 6. As we can see from Fig. 5, the standalone RF system consumes less power at the locations of the relay nodes while it requires more power at the location of $E$. The same power consumption pattern is applicable in the case of the hybrid RF/VLC system with a higher consumed power range. Moreover, it can be observed that the system consumes more power near the location of $E$ compared to the other locations of $D$, and this can be

[6] Note that the proposed algorithm aims to save as much as possible power after satisfying the required $\Delta_{\text{th}}$.

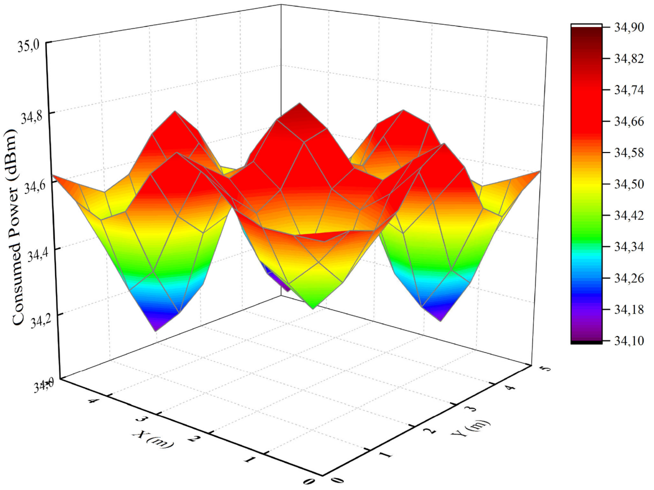


Fig. 5. The consumed power of the standalone RF system.

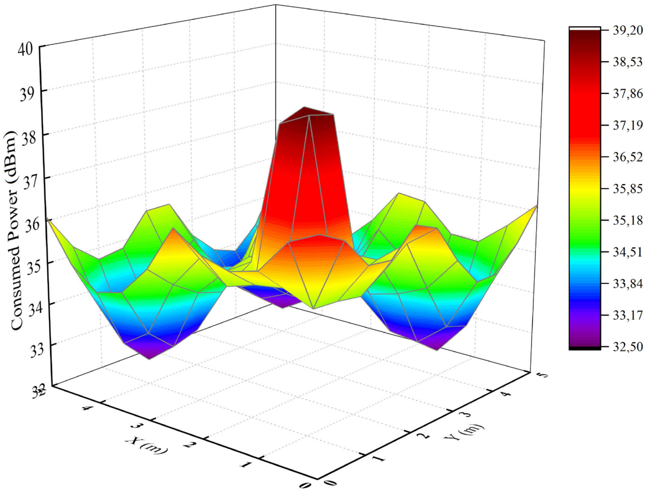


Fig. 6. The consumed power of the proposed hybrid RF/VLC relaying system.

explained by the fact that more power is needed since the relay selected according to (10) does not consider the location of $E$, and therefore further increase of the relay transmit power will increase the capacity of $E$.

Fig. 7 demonstrates the results on the achievable SC built versus the target SC threshold $\Delta_{\text{th}}$ for the standalone RF, standalone VLC and proposed hybrid (with and without jamming capabilities) systems where we fixed the location of $D$ at $(x = 4, y = 4, z = 1)$ m to make a fair comparison. To begin with, we consider the secrecy of the standalone VLC system which obtains maximum approx. 3.9 bits/s/Hz and starts saturating from $\Delta_{\text{th}} = 4$ bits/s/Hz. At the same time, the standalone RF system outperforms the previous one and can be characterized by a saturation of approx. 5.2 bits/s/Hz from $\Delta_{\text{th}} = 6$ bits/s/Hz. Next, we evaluate the SC of the proposed hybrid scheme which outperforms the both standalone systems and attains approximately 9 bits/s/Hz (see Fig. 7). The corresponding saturation starts at about $\Delta_{\text{th}} = 9.6$ bits/s/Hz. Finally, to prove the effectiveness of the proposed joint relay-jammer selection algorithm (implemented in all the aforementioned standalone and hybrid systems), we evaluate the impact of the jammer on the secrecy performance by considering the hybrid RF/VLC relaying system without jamming capabilities under the same

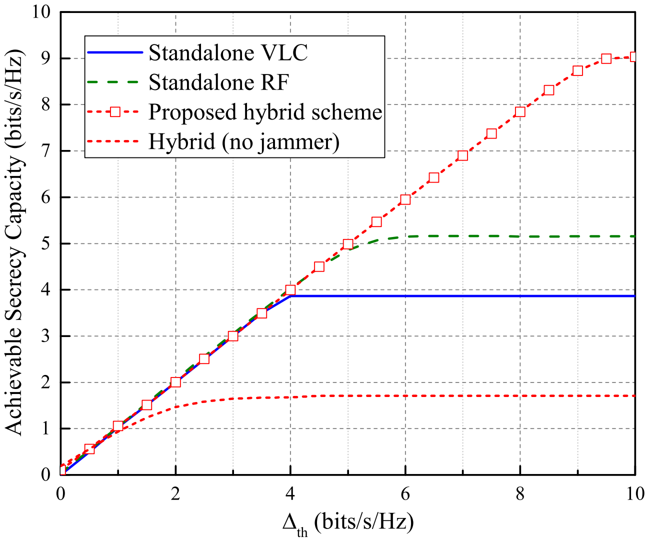


Fig. 7. The achievable secrecy performance versus the SC threshold.

system parameters. As we can see, the system performs worse due to the fact that the capacity of $E$ obtains higher values which consequently deteriorates the effective secrecy performance of the system, where it achieves approximately 1.6 bits/s/Hz and steady saturation from $\Delta_{\text{th}} = 4$ bits/s/Hz.

## 7. Conclusion

In this paper, we investigated the secrecy performance of the proposed hybrid RF/VLC network with multiple relays with jamming capabilities. We first proposed a novel joint relay-jammer selection scheme conditioned on the minimum outage and maximum SNR related to the selection of the relaying and jamming nodes, respectively. Next, beamforming vectors were designed for both RF and VLC subsystems to be used in the formulation of our power minimization problem. It was shown that the proposed technique outperforms all the other benchmark technologies and has a potential to support higher secrecy capacity. Finally, we proved the effectiveness of using the jammer as an eavesdropping-resilient PLS technique.

## References

[1] J. Reed, M. Vassiliou, and S. Shah, “The role of new technologies in solving the spectrum shortage,” *Proc. IEEE*, vol. 104, no. 6, pp. 1163–1168, Jun. 2016.

[2] H. Haas, L. Yin, Y. Wang, and C. Chen, “What is LiFi?” *J. Lightw. Technol.*, vol. 34, no. 6, pp. 1533–1544, Mar. 2016.

[3] A. Jovicic, J. Li, and T. Richardson, “Visible light communication: Opportunities, challenges and the path to market,” *IEEE Commun. Mag.*, vol. 51, no. 12, pp. 26–32, Dec. 2013.

[4] T. Komine and M. Nakagawa, “Fundamental analysis for visible-light communication system using LED lights,” *IEEE Trans. Consum. Electron.*, vol. 50, no. 1, pp. 100–107, Jun. 2004.

[5] H. Haas, “LiFi is a paradigm-shifting 5G technology,” *Rev. Phys.*, vol. 3, pp. 26–31, Nov. 2018.

[6] G. Nauryzbayev, M. Abdallah, and H. Elgala, “On the performance of NOMA-enabled spectrally and energy efficient OFDM (SEE-OFDM) for indoor visible light communications,” in *Proc. IEEE 87th Veh. Technol. Conf.*, Porto, Portugal, Jun. 2018, pp. 1–5.

[7] G. Nauryzbayev, M. Abdallah, and H. Elgala, “Outage of SEE-OFDM VLC-NOMA networks,” *IEEE Photon. Technol. Lett.*, vol. 31, no. 2, pp. 121–124, Jan. 15, 2019.

[8] P. K. Jha, N. Mishra, and D. S. Kumar, “Challenges and potentials for visible light communications: State of the art,” *Amer. Inst. Phys. Conf. Proc.*, vol. 1849, Jun. 2017, Art. no. 020007.

[9] M. Ayyash *et al.*, “Coexistence of WiFi and LiFi toward 5G: Concepts, opportunities, and challenges,” *IEEE Commun. Mag.*, vol. 54, no. 2, pp. 64–71, Feb. 2016.

[10] D. A. Basnayaka and H. Haas, “Hybrid RF and VLC systems: Improving user data rate performance of VLC systems,” in *Proc. IEEE 81st Veh. Technol. Conf.*, Jul. 2015, pp. 1–5.

[11] C. Yan, Y. Xu, J. Shen, and J. Chen, “A combination of VLC and WiFi based indoor wireless access network and its handover strategy,” in *Proc. IEEE Int. Conf. Ubiquitous Wireless Broadband*, Oct. 2016, pp. 1–4.

[12] R. Johri, “Li-Fi, complementary to Wi-Fi,” in *Proc. Int. Conf. Comput. Power, Energy Inf. Commun.*, Apr. 2016, pp. 15–19.

[13] X. Li, R. Zhang, and L. Hanzo, “Cooperative load balancing in hybrid visible light communications and WiFi,” *IEEE Trans. Commun.*, vol. 63, no. 4, pp. 1319–1329, Apr. 2015.

[14] M. Kashef, M. Ismail, M. Abdallah, K. A. Qaraqe, and E. Serpedin, “Energy efficient resource allocation for mixed RF/VLC heterogeneous wireless networks,” *IEEE J. Sel. Areas Commun.*, vol. 34, no. 4, pp. 883–893, Apr. 2016.

[15] J. Al-Khori, G. Nauryzbayev, M. Abdallah, and M. Hamdi, “Physical layer security for hybrid RF/VLC DF relaying systems,” in *Proc. IEEE Veh. Technol. Conf.*, Chicago, IL, USA, Aug. 2018, pp. 1–6.

[16] M. B. Rahaim, A. M. Vegni, and T. D. C. Little, “A hybrid radio frequency and broadcast visible light communication system,” in *Proc. IEEE Global Commun. Conf. Workshops*, Mar. 2011, pp. 792–796.

[17] J. Mo, M. Tao, and Y. Liu, “Relay placement for physical layer security: A secure connection perspective,” *IEEE Commun. Lett.*, vol. 16, no. 6, pp. 878–881, Jun. 2012.

[18] S. Arzykulov, G. Nauryzbayev, and T. A. Tsiftsis, “Underlay cognitive relaying system over $\alpha$-$\mu$ fading channels,” *IEEE Commun. Lett.*, vol. 21, no. 1, pp. 216–219, Jan. 2017.

[19] G. Nauryzbayev, S. Arzykulov, T. A. Tsiftsis, and M. Abdallah, “Performance of cooperative underlay CR-NOMA networks over Nakagami-$m$ channels,” in *Proc. IEEE Int. Conf. Commun. Workshops*, Kansas City, MO, USA, May 2018, pp. 1–6.

[20] S. Arzykulov, G. Nauryzbayev, T. A. Tsiftsis, and M. Abdallah, “Outage performance of underlay CR-NOMA networks,” in *Proc. 10th Int. Conf. Wireless Commun. Signal Process.*, Hangzhou, China, Oct. 2018, pp. 1–6.

[21] S. Arzykulov, T. A. Tsiftsis, G. Nauryzbayev, M. Abdallah, and G. Yang, “Outage performance of underlay CR-NOMA networks with detect-and-forward relaying,” in *Proc. IEEE Global Commun. Conf.*, Abu Dhabi, UAE, Dec. 2018, pp. 1–6.

[22] S. Arzykulov, G. Nauryzbayev, T. A. Tsiftsis, and M. Abdallah, “On the capacity of wireless powered cognitive relay network with interference alignment,” in *Proc. IEEE Global Commun. Conf.*, Dec. 2017, pp. 1–6.

[23] G. Nauryzbayev, K. M. Rabie, M. Abdallah, and B. Adebisi, “Ergodic capacity analysis of wireless powered AF relaying systems over $\alpha$-$\mu$ fading channels,” in *Proc. IEEE Global Commun. Conf.*, Dec. 2017, pp. 1–6.

[24] S. Arzykulov, G. Nauryzbayev, T. A. Tsiftsis, and M. Abdallah, “Error performance of wireless powered cognitive relay networks with interference alignment,” in *Proc. IEEE 28th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun.*, Oct. 2017, pp. 1–5.

[25] H. Yang and A. Pandharipande, “Full-duplex relay VLC in LED lighting triangular system topology,” in *Proc. 6th Int. Symp. Commun., Control Signal Process.*, May 2014, pp. 85–88.

[26] G. Nauryzbayev, K. M. Rabie, M. Abdallah, and B. Adebisi, “On the performance analysis of WPT-based dual-hop AF relaying networks in $\alpha$-$\mu$ fading,” *IEEE Access*, vol. 6, pp. 37138–37149, 2018.

[27] G. Nauryzbayev, M. Abdallah, and K. M. Rabie, “Outage probability of full-duplex AF and DF relaying systems over $\alpha$-$\mu$ channels,” in *Proc. IEEE Veh. Technol. Conf.*, Chicago, IL, USA, Aug. 2018, pp. 1–6.

[28] M. R. Zenaidi, Z. Rezki, M. Abdallah, K. A. Qaraqe, and M. S. Alouini, “Achievable rate-region of VLC/RF communications with an energy harvesting relay,” in *Proc. IEEE Global Commun. Conf.*, Dec. 2017, pp. 1–7.

[29] T. Rakia, H. C. Yang, F. Gebali, and M. S. Alouini, “Dual-hop VLC/RF transmission system with energy harvesting relay under delay constraint,” in *Proc. IEEE Global Commun. Workshops*, Dec. 2016 pp. 1–6.

[30] M. Masoud, I. Jannoud, A. Ahmad, and H. Al-Shobaky, “The power consumption cost of data encryption in smartphones,” in *Proc. Int. Conf. Open Source Softw. Comput.*, Sep. 2015, pp. 1–6.

[31] J. Wu, I. Detchenkov, and Y. Cao, “A study on the power consumption of using cryptography algorithms in mobile devices,” in *Proc. 7th IEEE Int. Conf. Softw. Eng. Serv. Sci.*, Aug. 2016, pp. 957–959.

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

[33] 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. Surv. Tut.*, vol. 16, no. 3, pp. 1550–1573, Feb. 2014.

[34] Y. Zou, J. Zhu, X. Wang, and V. C. M. Leung, “Improving physical-layer security in wireless communications using diversity techniques,” *IEEE Netw.*, vol. 29, no. 1, pp. 42–48, Feb. 2015.

[35] L. J. Rodriguez, N. H. Tran, T. Q. Duong, T. Le-Ngoc, M. Elkashlan, and S. Shetty, “Physical layer security in wireless cooperative relay networks: State of the art and beyond,” *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 32–39, Dec. 2015.

[36] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, “A survey on wireless security: Technical challenges, recent advances, and future trends,” *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[37] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, “Improving wireless physical layer security via cooperating relays,” *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[38] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, “Cooperative jamming for wireless physical layer security,” in *Proc. IEEE Workshop Statist. Signal Process.*, Sep. 2009, pp. 417–420.

[39] Y. Zou, X. Wang, and W. Shen, “Optimal relay selection for physical-layer security in cooperative wireless networks,” *IEEE J. Sel. Areas Commun.*, vol. 31, no. 10, pp. 2099–2111, Oct. 2013.

[40] Y. Liu, J. Li, and A. P. Petropulu, “Destination assisted cooperative jamming for wireless physical-layer security,” *IEEE Trans. Inf. Forensics Secur.*, vol. 8, no. 4, pp. 682–694, Apr. 2013.

[41] L. Yin and H. Haas, “Physical-layer security in multiuser visible light communication networks,” *IEEE J. Sel. Areas Commun.*, vol. 36, no. 1, pp. 162–174, Jan. 2018.

[42] H. Shen, Y. Deng, W. Xu, and C. Zhao, “Rate-maximized zero-forcing beamforming for VLC multiuser MISO downlinks,” *IEEE Photon. J.*, vol. 8, no. 1, Feb. 2016, Art. no. 7901913.

[43] S. Cho, G. Chen, and J. P. Coon, “Securing visible light communication systems by beamforming in the presence of randomly distributed eavesdroppers,” *IEEE Trans. Wireless Commun.*, vol. 17, no. 5, pp. 2918–2931, May 2018.

[44] A. Mostafa and L. Lampe, “Securing visible light communications via friendly jamming,” in *Proc. IEEE Global Commun. Conf.*, Dec. 2014, pp. 524–529.

[45] J. Al-Khori, G. Nauryzbayev, M. Abdallah, and M. Hamdi, “Secrecy Capacity of Hybrid RF/VLC DF Relaying Networks with Jamming,” in *Proc. Int. Conf. Comput., Netw. Commun.*, Honolulu, HI, USA, Feb. 2019, pp. 1–6.
[46] J. Al-Khori, G. Nauryzbayev, M. M. Abdallah, and M. Hamdi, “Secrecy performance of decode-and-forward based hybrid RF/VLC relaying systems,” *IEEE Access*, vol. 7, pp. 10844–10856, 2019.
[47] M. F. Marzban, M. Kashef, M. Abdallah, and M. Khairy, “Beamforming and power allocation for physical-layer security in hybrid RF/VLC wireless networks,” in *Proc. 13th Int. Wireless Commun. Mobile Comput. Conf.*, Jun. 2017, pp. 258–263.
[48] L. Dong, H. Yousefi’zadeh, and H. Jafarkhani, “Cooperative jamming and power allocation for wireless relay networks in presence of eavesdropper,” in *Proc. Int. Conf. Commun.*, Jun. 2011, pp. 1–6.
[49] K. H. Park, T. Wang, and M.-S. Alouini, “On the jamming power allocation for secure amplify-and-forward relaying via cooperative jamming,” *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1741–1750, Sep. 2013.
[50] H. Zaid, Z. Rezki, A. Chaaban, and M.-S. Alouini, “Improved achievable secrecy rate of visible light communication with cooperative jamming,” in *Proc. IEEE Global Conf. Signal Inf. Process.*, Dec. 2015, pp. 1165–1169.
[51] A. Mostafa and L. Lampe, “Securing visible light communications via friendly jamming,” in *Proc. IEEE Global Commun. Conf. Workshops*, Dec. 2014, pp. 524–529.
[52] M. Kang and M. S. Alouini, “A comparative study on the performance of MIMO MRC systems with and without co-channel interference,” *IEEE Trans. Commun.*, vol. 52, no. 8, pp. 1417–1425, Aug. 2004.
[53] S. Boyd and L. Vandenberghe, *Convex Optimization*, 7th ed. Cambridge, U.K.: Cambridge Univ. Press, 2004.
[54] F. Oggier and B. Hassibi, “The secrecy capacity of the MIMO wiretap channel,” *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.
[55] S. Leung-Yan-Cheong and M. Hellman, “The Gaussian wire-tap channel,” *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451–456, Jul. 1978.