Relay-Aided Secure Broadcasting for VLC

Ahmed Arafa[1], Erdal Panayirci[2,1], and H. Vincent Poor[1]

[1]Electrical Engineering Department, Princeton University, USA
[2]Department of Electrical and Electronics Engineering, Kadir Has University, Istanbul, Turkey

***Abstract*— A visible light communication (VLC) broadcast channel is considered, in which a transmitter communicates with two receivers in the presence of an external eavesdropper. Trusted cooperative half-duplex relays are deployed to aid with securing the transmitted data. Transmission is amplitude-constrained to maintain operation within the light emitting diodes (LEDs) dynamic range. Achievable secrecy rate regions are derived under such amplitude constraints for this multi receiver wiretap channel, first for direct transmission without the relays, and then for *cooperative jamming*, *decode-and-forward*, and *amplify-and-forward* relaying schemes. Superposition coding with uniform signaling is used for transmission, along with *secure beamforming* at the relays. Superiority of the secure relaying schemes over direct transmission is shown, with performance depending on how far the eavesdropper is from the transmitter and the relays.**

I. Introduction

VLC technology is a promising candidate for future high-speed communication systems, offering solutions to spectrum congestion issues in conventional radio frequency systems [1], [2]. The broadcast property in VLC, however, calls for careful design of secure communications to protect legitimate users from potential eavesdroppers, especially in public areas. Physical layer security is a powerful technique to deliver, provably, secure data, see, e.g., [3]. In this work, we design physical layer secure relaying schemes for a broadcast VLC channel with an external eavesdropper.

Recently, there have been several works on physical layer security aspects in VLC, see, e.g., [4]–[20]. References [19], [20] are the most closely related to our work, in which broadcast VLC channels with confidential messages are considered. Relaying in VLC has been previously studied in [21].

In this paper, we investigate the role of trusted cooperative half-duplex relays in securing a two-user broadcast VLC channel from an external eavesdropper. An amplitude constraint is imposed upon the transmitted signal for the LEDs to operate within their dynamic range. Under such amplitude constraint, we derive an achievable secrecy rate region based on superposition coding with uniform signaling. We then invoke the relays, and derive several achievable secrecy rate regions via *cooperative jamming*, *decode-and-forward*, and *amplify-and-forward* schemes. For each scheme, we design *secure beamforming* vectors to maximize the achievable rates. Results show the enhancement of the achievable rates using the relays, and that the best relaying scheme is a function of the eavesdropper's distance from the transmitter and the relays.

This research was supported in part by the U.S. National Science Foundation under Grant CNS-1702808.

Erdal Panayirci has been supported by the Turkish Scientific and Research Council (TUBITAK) under 2219 International Fellowship Program and in part by KAUST under Grant No. OSR-2016-CRG5-2958-02.

II. System Model

We consider an indoor VLC channel in which a transmitter (source) communicates with two legitimate receivers (users) in the presence of an external eavesdropper. The source is mounted on the ceiling, and is equipped with one light fixture that contains multiple LEDs modulated by the same current signal. The two users, and the eavesdropper, are assumed to lie geometrically on a two-dimensional plane close to the floor, and are each equipped with a single photo detector (PD).

The source's LEDs are driven by a fixed, positive bias current that sets the illumination intensity. The data signal, $x \in \mathbb{R}$, is superimposed on the bias current to modulate the instantaneous optical power emitted from the LEDs. The source uses superposition coding [22] to transmit two messages x_1 and x_2 to the first and the second user, respectively, by setting

$$x = \alpha x_1 + (1-\alpha)x_2 \tag{1}$$

for some $\alpha \in [0,1]$ that determines the priority of each user. In order to avoid clipping distortion and to maintain operation within the LEDs' dynamic range, an amplitude constraint, $A > 0$, is enforced as follows:

$$\alpha|x_1| + (1-\alpha)|x_2| \leq A \quad \text{a.s.} \tag{2}$$

Let h_1, h_2, and h_e denote the positive channel gains between the source and the first user, second user, and eavesdropper, respectively. h_1 and h_2 are known at the source. Without loss of generality, let $h_1 > h_2$, and hence the first (strong) user decodes the second (weak) user's message first, then uses successive interference cancellation to decode its own message, while the weak user decodes its message by treating the strong user's interfering signal as noise [22]. y_1, y_2, and y_e, denoting the received signals, in the electric domain, at the strong user, weak user, and eavesdropper, respectively, are

$$y_j = h_j x + n_j, \quad j = 1, 2, e, \tag{3}$$

where n_1, n_2, and n_e are i.i.d. $\sim \mathcal{N}(0,1)$ noise terms.

Let there be K trusted cooperative half-duplex relay nodes. These can be, e.g., on the walls of the room, or hanging from the ceiling in between the source and the users. Source-relays channel gains are denoted by the vector[1] $\boldsymbol{h}_r$, and $\boldsymbol{g}_1$, $\boldsymbol{g}_2$, and $\boldsymbol{g}_e$ denote the channel gain vectors from the relays to the strong user, weak user, and eavesdropper, respectively. $\boldsymbol{g}_1$, $\boldsymbol{g}_2$, and $\boldsymbol{g}_e$ are known at the relays. An amplitude constraint, $\bar{A} > 0$, applies to the each relay's transmitted signal.

[1]All vectors in this paper are column vectors.

III. Direct Transmission

In this section, we derive an achievable secrecy rate region via direct transmission, i.e., without using the relay nodes. We state the result in Theorem 1 below[2].

Theorem 1 *The following secrecy rate pair*[3] *is achievable via direct transmission for a given* α*:*

$$r_{1,s}=\left[\frac{1}{2}\log\left(1+\frac{2h_1^2\alpha^2A^2}{\pi e}\right)-\frac{1}{2}\log\left(1+\frac{h_e^2\alpha^2A^2}{3}\right)\right]^+, \quad (4)$$

$$r_{2,s}=\left[\frac{1}{2}\log\left(\frac{1+\frac{2h_2^2A^2}{\pi e}}{1+\frac{h_2^2\alpha^2A^2}{3}}\right)-\frac{1}{2}\log\left(\frac{1+\frac{h_e^2A^2}{3}}{1+\frac{2h_e^2\alpha^2A^2}{\pi e}}\right)\right]^+. \quad (5)$$

The proof of Theorem 1 mainly follows by lower bounding the capacity achieving superposition coding rates for this multi receiver wiretap channel, reported in [24], via uniform signaling on $[-A, A]$. Taking the union over α gives the full secrecy rate region. Observe that for $\alpha = 1$, we get that $r_{2,s} = 0$ since $\frac{2}{\pi e} < \frac{1}{3}$, and $r_{1,s}$ coincides with the SISO achievable rate derived in [5], since the signal now is only directed towards the strong user. The opposite holds for $\alpha = 0$ as well. It is also clear from (4) and (5) that the strong user's achievable secrecy rate is positive if and only if (iff) $\frac{2}{\pi e}h_1^2 > \frac{1}{3}h_e^2$, and that the weak user's achievable secrecy rate is positive iff $\left(\frac{2}{\pi e}-\frac{\alpha^2}{3}\right)h_2^2+\left(\frac{2\alpha^2}{\pi e}-\frac{1}{3}\right)h_e^2 > \left(\frac{1}{9}-\frac{4}{\pi^2e^2}\right)\alpha^2h_2^2h_e^2$. Thus, achieving positive secrecy rates depends on the relative channel conditions between the users and the eavesdropper.

IV. Cooperative Jamming

In this section, we discuss the cooperative jamming scheme. In such, the relays cooperatively transmit a jamming signal $\boldsymbol{J}z$, *simultaneously* with the source's transmission, to confuse the eavesdropper. Here, $\boldsymbol{J} \in \mathbb{R}^K$ is a beamforming vector and z is a random variable satisfying the following constraints:

$$|z| \le \bar{A} \quad \text{a.s.}, \qquad |\boldsymbol{J}| \preceq \mathbf{1}_K, \quad (6)$$

where $\mathbf{1}_K$ is an all-ones K-length vector, and the inequality $\preceq$ is element-wise. The received signals at the legitimate users and the eavesdropper are now given by

$$y_j = h_j x + \boldsymbol{g}_j^T\boldsymbol{J}z + n_j, \quad j = 1, 2, e, \quad (7)$$

where the superscript T denotes the transpose operation.

In order not to harm the legitimate users, the beamforming vector is designed such that: $\boldsymbol{g}_1^T\boldsymbol{J} = \boldsymbol{g}_2^T\boldsymbol{J} = 0$, which is guaranteed if $K \ge 3$ relays, making the matrix $\boldsymbol{G}^T \triangleq [\boldsymbol{g}_1\ \boldsymbol{g}_2]^T$ have a non-empty null space. We denote such beamforming vector by $\boldsymbol{J}_o$. We now state the cooperative jamming result.

Theorem 2 *The following secrecy rate pair is achievable via cooperative jamming for a given* α*:*

$$r_{1,s}^J = \left[\frac{1}{2}\log\left(1+\frac{2h_1^2\alpha^2A^2}{\pi e}\right) - \frac{1}{2}\log\left(\frac{1+\frac{h_e^2\alpha^2A^2}{3}+\frac{\left(\boldsymbol{g}_e^T\boldsymbol{J}_o\right)^2\bar{A}^2}{3}}{1+\frac{2(\boldsymbol{g}_e^T\boldsymbol{J}_o)^2\bar{A}^2}{\pi e}}\right)\right]^+, \quad (8)$$

$$r_{2,s}^J = \left[\frac{1}{2}\log\left(\frac{1+\frac{2h_2^2A^2}{\pi e}}{1+\frac{h_2^2\alpha^2A^2}{3}}\right) - \frac{1}{2}\log\left(\frac{1+\frac{h_e^2A^2}{3}+\frac{\left(\boldsymbol{g}_e^T\boldsymbol{J}_o\right)^2\bar{A}^2}{3}}{1+\frac{2h_e^2\alpha^2A^2}{\pi e}+\frac{2(\boldsymbol{g}_e^T\boldsymbol{J}_o)^2\bar{A}^2}{\pi e}}\right)\right]^+. \quad (9)$$

The proof of Theorem 2 follows via similar approaches as in the proof of Theorem 1, with the random variable z being uniformly distributed on $\left[-\bar{A}, \bar{A}\right]$. We now proceed to find the optimal beamforming vector $\boldsymbol{J}_o$ that maximally degrades the eavesdropper's channel. In view of (8) and (9), by direct first derivative analysis, one can show that $r_{1,s}^J$ is increasing in $\left(\boldsymbol{g}_e^T\boldsymbol{J}_o\right)^2$ iff $h_e^2\alpha^2A^2 > \frac{\pi e}{2} - 3 \approx 1.27$. Similarly, $r_{2,s}^J$ is increasing in $\left(\boldsymbol{g}_e^T\boldsymbol{J}_o\right)^2$ iff $h_e^2\left(1-\alpha^2\right)A^2 > 1.27$. We note that, as a direct consequence of the data processing inequality [22], sending a jamming signal can only degrade the eavesdropper's channel. It is clear, however, that the previous two inequalities do not hold all the time, and hence sending a jamming signal might actually benefit the eavesdropper. This is justified though since we only derive a lower bound on the achievable secrecy rate, as opposed to exact computations. Whenever the secrecy rate (of either user) is increasing in $\left(\boldsymbol{g}_e^T\boldsymbol{J}_o\right)^2$, we find the optimal beamforming vector $\boldsymbol{J}_o^*$ by solving the following optimization problem:

$$\max_{\boldsymbol{J}_o} \quad \left(\boldsymbol{g}_e^T\boldsymbol{J}_o\right)^2$$
$$\text{s.t.} \quad \boldsymbol{G}^T\boldsymbol{J}_o = \begin{bmatrix}0 & 0\end{bmatrix}, \quad |\boldsymbol{J}_o| \preceq \mathbf{1}_K. \quad (10)$$

To solve the above, the optimal $\boldsymbol{J}_o^*$ vector should then be of the form: $\boldsymbol{J}_o^* = \mathcal{P}^\perp(\boldsymbol{G})\,\boldsymbol{u}_J$, for some vector $\boldsymbol{u}_J \in \mathbb{R}^K$, where $\mathcal{P}^\perp(\boldsymbol{A}) \triangleq \boldsymbol{I}_K - \boldsymbol{A}\left(\boldsymbol{A}^T\boldsymbol{A}\right)^{-1}\boldsymbol{A}^T$ is the projection matrix onto the null space of a matrix $\boldsymbol{A} \in \mathbb{R}^{K\times K}$ with $\boldsymbol{I}_K$ denoting the $K \times K$ identity matrix[4]. Choosing $\boldsymbol{u}_J = c_J\boldsymbol{g}_e$ maximizes the objective function of problem (10) for some constant $c_J \in \mathbb{R}$. To satisfy the amplitude constraint, we choose c_J such that

$$\boldsymbol{J}_o^* = \frac{\mathcal{P}^\perp(\boldsymbol{G})\,\boldsymbol{g}_e}{\max_i\left(|\mathcal{P}^\perp(\boldsymbol{G})\,\boldsymbol{g}_e|\right)_i}, \quad (11)$$

where $(\boldsymbol{l})_i$ denotes the ith component of a vector $\boldsymbol{l}$.

V. Decode-and-Forward

In this section, we discuss the decode-and-forward scheme. Communication occurs over two phases. In the first phase, the source broadcasts its messages to both the legitimate users and relays. In the second phase, the relays decode the received messages and forward them to the users. The eavesdropper overhears the transmission over the two phases.

The received signal at the relays in the first phase is

$$\boldsymbol{y}_r = \boldsymbol{h}_r x + \boldsymbol{n}_r, \quad (12)$$

[2]Detailed proofs are stated in [23] and are omitted here due to space limits.

[3]$\log$ denotes natural logarithm, and $[\cdot]^+ \triangleq \max(\cdot, 0)$.

[4]Note that $\mathcal{P}^\perp$ can be defined to operate on vectors as well, denoting a projection onto their orthogonal complements in the space.

where $\boldsymbol{n}_r \sim \mathcal{N}(\boldsymbol{0}, \boldsymbol{I}_K)$ represents the Gaussian noise in the source-relays channels. In the second phase, the ith relay decodes its received signal to get x_1 and x_2, re-encodes them into $\tilde{x}_1$ and $\tilde{x}_2$, respectively, using independent codewords, and forwards them to the users using superposition coding. Let $\boldsymbol{d}x_r$ denote the relays' transmitted signals, where $\boldsymbol{d} \triangleq [d_1, d_2, \ldots, d_K]$ is a beamforming vector and $x_r \triangleq \alpha\tilde{x}_1 + (1-\alpha)\tilde{x}_2$. The following constraints now hold at the relays:

$$\alpha|\tilde{x}_1| + (1-\alpha)|\tilde{x}_2| \leq \bar{A} \quad \text{a.s.}, \qquad |\boldsymbol{d}| \preceq \boldsymbol{1}_K. \tag{13}$$

The received signals at the legitimate users and the eavesdropper in the second phase are given by

$$y_j^r = \boldsymbol{g}_j^T \boldsymbol{d} x_r + n_j^r, \quad j = 1, 2, e, \tag{14}$$

where the superscript r is to denote relay-received signals, and the noise terms n_1^r, n_2^r, and n_e^r are i.i.d. $\sim \mathcal{N}(0,1)$.

For $K \geq 2$ relays, we propose designing the beamforming vector $\boldsymbol{d}$ to satisfy the following: $\boldsymbol{g}_e^T \boldsymbol{d} = 0$, so that the eavesdropper does not receive any useful information in the second phase. We denote such beamforming vector by $\boldsymbol{d}_o$. If $K \geq 3$ relays, then it holds that both $\boldsymbol{g}_1^T \boldsymbol{d}_o$ and $\boldsymbol{g}_2^T \boldsymbol{d}_o$ are non-zero. We now state the decode-and-forward result.

Theorem 3 *The following secrecy rate pair is achievable via decode-and-forward for a given α:*

$$r_{1,s}^{DF} = \frac{1}{2}\left[r_1^{DF} - \frac{1}{2}\log\left(1 + \frac{h_e^2\alpha^2 A^2}{3}\right)\right]^+ \tag{15}$$

$$r_{2,s}^{DF} = \frac{1}{2}\left[r_2^{DF} - \frac{1}{2}\log\left(\frac{1 + \frac{h_e^2 A^2}{3}}{1 + \frac{2h_e^2\alpha^2 A^2}{\pi e}}\right)\right]^+ \tag{16}$$

with r_1^{DF} and r_2^{DF} given by (17) and (18), respectively.

The proof of Theorem 3 follows by evaluating the decode-and-forward lower bound in [25, Theorem 16.2] with uniform signaling, followed by similar lower-bounding approaches as in the proof of Theorem 1. The extra $\frac{1}{2}$ terms are due to sending the same message over two phases of equal durations. In view of (17) and (18), we see that r_1^{DF} is increasing in $\left(\boldsymbol{g}_1^T \boldsymbol{d}_o\right)^2$, while direct first derivative analysis shows that r_2^{DF} is increasing in $\left(\boldsymbol{g}_1^T \boldsymbol{d}_o\right)^2$ iff $\alpha \leq \sqrt{\frac{2/\pi e}{1/3}} \approx 0.838$, yet this condition can be ignored since $r_{s,2}^{DF}$ can only be positive if $\alpha \leq 0.838$. Therefore, we propose the following optimization problem to find the best beamforming vector:

$$\begin{aligned} \max_{\boldsymbol{d}_o} \quad & \alpha\left(\boldsymbol{g}_1^T \boldsymbol{d}_o\right)^2 + (1-\alpha)\left(\boldsymbol{g}_2^T \boldsymbol{d}_o\right)^2 \\ \text{s.t.} \quad & \boldsymbol{g}_e^T \boldsymbol{d}_o = 0, \quad |\boldsymbol{d}_o| \preceq \boldsymbol{1}_K. \end{aligned} \tag{19}$$

Whence, the optimal $\boldsymbol{d}_o^*$ should be of the form: $\boldsymbol{d}_o^* = \mathcal{P}^{\perp}(\boldsymbol{g}_e)\,\boldsymbol{u}_d \triangleq \boldsymbol{F}_d \boldsymbol{u}_d$, for some vector $\boldsymbol{u}_d \in \mathbb{R}^K$. To choose the best $\boldsymbol{u}_d$, we rewrite the objective function of the above problem slightly differently as: $\boldsymbol{u}_d^T \boldsymbol{F}_d \left(\alpha \boldsymbol{g}_1 \boldsymbol{g}_1^T + (1-\alpha)\boldsymbol{g}_2 \boldsymbol{g}_2^T\right) \boldsymbol{F}_d \boldsymbol{u}_d$, and therefore, the optimal $\boldsymbol{u}_d$ is given by $\boldsymbol{u}_d = c_d \boldsymbol{v}_d$, where $c_d \in \mathbb{R}$ is a constant, and $\boldsymbol{v}_d$ is the leading eigenvector of the matrix $\boldsymbol{F}_d \left(\alpha \boldsymbol{g}_1 \boldsymbol{g}_1^T + (1-\alpha)\boldsymbol{g}_2 \boldsymbol{g}_2^T\right) \boldsymbol{F}_d$, i.e., the eigenvector corresponding to the largest eigenvalue of the matrix. We choose c_d to satisfy the amplitude constraint as follows:

$$\boldsymbol{d}_o^* = \frac{\boldsymbol{F}_d \boldsymbol{v}_d}{\max_i \left(|\boldsymbol{F}_d \boldsymbol{v}_d|\right)_i}. \tag{20}$$

VI. Amplify-and-Forward

In this section, we discuss the amplify-and-forward scheme. Communication also occurs over two phases. In the second phase, however, the ith relay merely re-sends its received signal from the first phase after multiplying (amplifying) it by a constant $a_i \in \mathbb{R}$ to be designed. Effectively, the relays' transmitted signal in the second phase is given by $\texttt{diag}\left(\boldsymbol{y}_r\right)\boldsymbol{a}$, where $\texttt{diag}(\boldsymbol{l})$ is the diagonalization of a vector $\boldsymbol{l}$. The following amplitude constraint holds at the relays:

$$|\texttt{diag}\left(\boldsymbol{y}_r\right)\boldsymbol{a}| \preceq \boldsymbol{1}_K \bar{A} \quad \text{a.s.} \tag{21}$$

The received signals in the second phase are given by

$$y_j^r = \boldsymbol{g}_j^T \texttt{diag}\left(\boldsymbol{y}_r\right)\boldsymbol{a} + n_j^r, \quad j = 1, 2, e. \tag{22}$$

As in the decode-and-forward case, we design the beamforming vector $\boldsymbol{a}$ to satisfy: $\boldsymbol{g}_e^T \texttt{diag}\left(\boldsymbol{h}_r\right)\boldsymbol{a} = 0$, so that the eavesdropper does not receive useful information in the second phase, and denote it by $\boldsymbol{a}_o$. We now state the amplify-and-forward result.

Theorem 4 *The following secrecy rate pair is achievable via amplify-and-forward for a given α:*

$$r_{1,s}^{AF} = \frac{1}{2}\left[\frac{1}{2}\log\left(1 + \frac{2\kappa_1^2\alpha^2 A^2}{\pi e}\right) - \frac{1}{2}\log\left(1 + \frac{h_e^2\alpha^2 A^2}{3}\right)\right]^+, \tag{23}$$

$$r_{2,s}^{AF} = \frac{1}{2}\left[\frac{1}{2}\log\left(\frac{1 + \frac{2\kappa_2^2 A^2}{\pi e}}{1 + \frac{\kappa_2^2\alpha^2 A^2}{3}}\right) - \frac{1}{2}\log\left(\frac{1 + \frac{h_e^2 A^2}{3}}{1 + \frac{2h_e^2\alpha^2 A^2}{\pi e}}\right)\right]^+, \tag{24}$$

where $\kappa_j^2 \triangleq h_j^2 + \frac{\left(\boldsymbol{g}_j^T \texttt{diag}(\boldsymbol{h}_r)\boldsymbol{a}_o\right)^2}{1 + \left(\boldsymbol{g}_j^T \boldsymbol{a}_o\right)^2}$, $j = 1, 2$.

The proof of Theorem 4 follows by viewing the system as a 1×2 SIMO system and applying the capacity achieving maximal ratio combining to get a sufficient statistic [26], followed by similar lower-bounding approaches as in the proof of Theorem 1. In view of (23) and (24), we see that $r_{1,s}^{AF}$ is increasing in κ_1^2, while direct first derivative shows that $r_{2,s}^{AF}$ is increasing in κ_2^2 iff $\alpha \leq 0.838$, yet again this condition can be ignored since $r_{2,s}^{AF}$ can only be positive if $\alpha \leq 0.838$. Thus, we solve the following optimization problem to find the best beamforming vector that maximizes jth user's rate, $j = 1, 2$:

$$\begin{aligned} \max_{\boldsymbol{a}_o} \quad & \frac{\left(\boldsymbol{g}_j^T \texttt{diag}\left(\boldsymbol{h}_r\right)\boldsymbol{a}_o\right)^2}{1 + \left(\boldsymbol{g}_j^T \boldsymbol{a}_o\right)^2} \\ \text{s.t.} \quad & \boldsymbol{g}_e^T \texttt{diag}\left(\boldsymbol{h}_r\right)\boldsymbol{a}_o = 0, \ |\texttt{diag}\left(\boldsymbol{y}_r\right)\boldsymbol{a}_o| \preceq \boldsymbol{1}_K \bar{A}. \end{aligned} \tag{25}$$

To solve (25), consider the following auxilliary problem:

$$\begin{aligned} p_j^a(\lambda) \triangleq \max_{\boldsymbol{a}_o} \quad & \left(\boldsymbol{g}_j^T \texttt{diag}\left(\boldsymbol{h}_r\right)\boldsymbol{a}_o\right)^2 - \lambda\left(1 + \left(\boldsymbol{g}_j^T \boldsymbol{a}_o\right)^2\right) \\ \text{s.t.} \quad & \text{problem (25)'s constraints} \end{aligned} \tag{26}$$

$$r_1^{DF} = \min\left\{\frac{1}{2}\log\left(1+\frac{2h_1^2\alpha^2A^2}{\pi e}\right)+\frac{1}{2}\log\left(1+\frac{2\left(\boldsymbol{g}_1^T\boldsymbol{d}_o\right)^2\alpha^2\bar{A}^2}{\pi e}\right), \frac{1}{2}\log\left(1+\min_{1\le i\le K}\frac{2h_{r,i}^2\alpha^2A^2}{\pi e}\right)\right\} \quad (17)$$

$$r_2^{DF} = \min\left\{\frac{1}{2}\log\left(\frac{1+\frac{2h_2^2A^2}{\pi e}}{1+\frac{h_2^2\alpha^2A^2}{3}}\right)+\frac{1}{2}\log\left(\frac{1+\frac{2\left(\boldsymbol{g}_2^T\boldsymbol{d}_o\right)^2\bar{A}^2}{\pi e}}{1+\frac{\left(\boldsymbol{g}_2^T\boldsymbol{d}_o\right)^2\alpha^2\bar{A}^2}{3}}\right), \frac{1}{2}\log\left(\min_{1\le i\le K}\frac{1+\frac{2h_{r,i}^2A^2}{\pi e}}{1+\frac{h_{r,i}^2\alpha^2A^2}{3}}\right)\right\} \quad (18)$$

for some $\lambda \geq 0$. One can show the following: 1) $p_j^a(\lambda)$ is decreasing in λ; and 2) the optimal solution of problem (25) is given by λ^* that solves $p_j^a(\lambda^*) = 0$ [27]. Hence, one can find an upper bound on λ^* that makes $p_j^a(\lambda) < 0$ and then proceed by, e.g., a bisection search to find λ^*. Focusing on problem (26), one can proceed as in the decode-and-forward case to conclude that the optimal $\boldsymbol{a}_o^{(j)}$ should be of the form

$$\boldsymbol{a}_o^{(j)} = \frac{\boldsymbol{F}_a\boldsymbol{v}_a^{(j)}}{\max_i\left(\left|\mathtt{diag}\left(\boldsymbol{g}_r\right)\boldsymbol{F}_a\boldsymbol{v}_a^{(j)}\right|\right)_i}\bar{A}, \quad (27)$$

where $\boldsymbol{F}_a \triangleq \mathcal{P}^{\perp}(\mathtt{diag}\left(\boldsymbol{h}_r\right)\boldsymbol{g}_e)$, and $\boldsymbol{v}_a^{(j)}$ is the leading eigenvector of the matrix $\boldsymbol{F}_a\left(\mathtt{diag}\left(\boldsymbol{h}_r\right)\boldsymbol{g}_j\boldsymbol{g}_j^T\mathtt{diag}\left(\boldsymbol{h}_r\right)-\lambda\boldsymbol{g}_j\boldsymbol{g}_j^T\right)\boldsymbol{F}_a$. Finally, we propose using the following beamforming vector: $\boldsymbol{a}_o^* = \alpha\boldsymbol{a}_o^{(1)} + (1-\alpha)\boldsymbol{a}_o^{(2)}$.

VII. Numerical Evaluations

We now validate our results via numerical evaluations. Consider a room of size $5\times5\times3$ m^3. The source is located at $(0,0,3)$, the strong user at $(0.75,0.75,0.7)$, and the weak user at $(-1.25,0.75,0.7)$. $K=5$ relays are located at the following positions: $(0.1,0.1,2)$, $(0.1,-0.1,2)$, $(0,0,2)$, $(-0.1,0.1,2)$, and $(-0.1,-0.1,2)$. The channel gain between two nodes q_1 and q_2 is given by [28]: $\frac{A_{det}(m+1)}{2\pi l_{q_1,q_2}^2}\left(\frac{|z_{q_1}-z_{q_2}|}{l_{q_1,q_2}}\right)^{m+1}$, where $A_{det} = 10^{-4}$ m^2 is the PD's physical area, $m = -\log(2)/\log\left(\cos\phi_{\frac{1}{2}}\right)$ is the order of Lambertian emission, with $\phi_{\frac{1}{2}} = 60^{\circ}$ denoting the LED semi-angle at half power, l_{q_1,q_2} is the distance between the two nodes, and z_j is the third coordinate of the jth node location. We set[5] $A = 10^7$ and $\bar{A} = 10^6$. We also ignore optimizing the term λ in the amplify-and-forward scheme for simplicity, and set it to 1.

In Fig. 1, we plot the achievable secrecy rate regions of the schemes proposed in this paper. Solid lines are when the eavesdropper is at $(0,1.65,0.7)$. In this case, all proposed schemes perform better than direct transmission. Dashed lines in Fig. 1 are when the eavesdropper is a bit further away from the source and the relays at $(0,2,0.7)$, in which case higher secrecy rates are achievable, yet both the decode-and-forward and amplify-and-forward schemes perform worse than direct transmission, since the channels from the relays to the eavesdropper are relatively worse, and hence the $\frac{1}{2}$ terms due to the half-duplex operation become more dominant than the gain due to beamforming. We also notice the improvement of the cooperative jamming scheme in this case over direct transmission. Fig. 1 shows that the best relaying scheme depends on the distance to the eavesdropper.

[5]Since noise power is normalized, note that the signal-to-noise ratio is represented by the square of the amplitude multiplied by the channel gain.

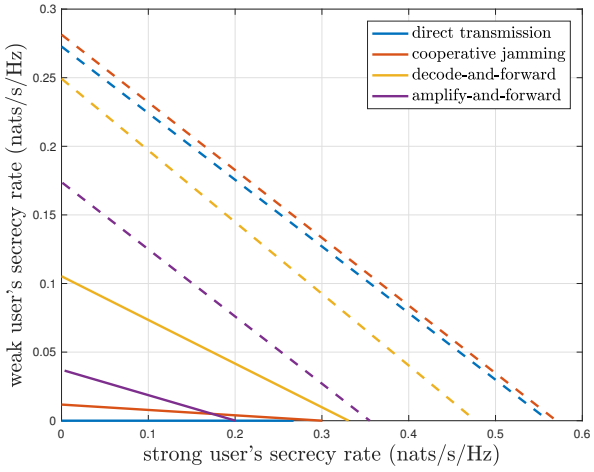

Fig. 1. Achievable secrecy regions of the proposed schemes. Solid lines are with eavesdropper at $(0,1.65,0.7)$, and dashed lines are with it at $(0,2,0.7)$.

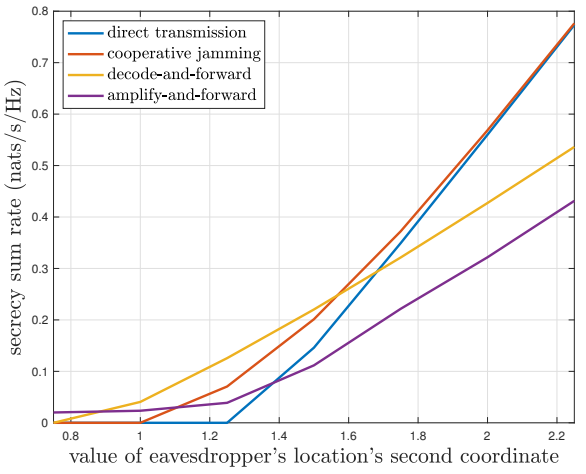

Fig. 2. Effect of eavesdropper's distance from the source on the achievable secrecy sum rate with $\alpha = 0.8$.

In Fig. 2, we focus on the effect of the eavesdropper's distance from the source on the secrecy sum rate for a fixed $\alpha = 0.8$. We vary the eavesdropper's location from $(0,0.75,0.7)$ to $(0,2.25,0.7)$, and observe from the figure that while the sum secrecy rate increases, for all schemes, as the eavesdropper's distance from the source increases, the proposed relaying schemes achieve strictly positive rates, as opposed to the zero rate achieved via direct transmission, at relatively closer locations to the source.

REFERENCES

[1] T. Komine and M. Nakagawa. Fundamental analysis for visible-light communication system using LED lights. *IEEE Trans. Consum. Electron.*, 50(1):100–107, February 2004.

[2] J. Grubor, K. Langer, J. W. Walewski, and S. Randel. High-speed wireless indoor communication via visible light. *ITG Fachericht*, 198:203–208, 2007.

[3] H. V. Poor and R. F. Schaefer. Wireless physical layer security. *Proc. National Academy of Sciences of USA*, 114(1):19–26, January 2017.

[4] A. Mostafa and L. Lampe. Securing visible light communications via friendly jamming. In *Proc. IEEE Globecom*, December 2014.

[5] A. Mostafa and L. Lampe. Physical-layer security for MISO visible light communication channels. *IEEE Trans. Commun.*, 33(9):1806–1818, September 2015.

[6] H. Zaid, Z. Rezki, A. Chaaban, and M. S. Alouini. Improved achievable secrecy rate of visible light communication with cooperative jamming. In *Proc. IEEE GlobalSIP*, December 2015.

[7] A. Mostafa and L. Lampe. Optimal and robust beamforming for secure transmission in MISO visible-light communication links. *IEEE Trans. Signal Process.*, 64(24):6501–6516, December 2016.

[8] M. A. Arfaoui, Z. Rezki, A. Ghrayeb, and M. S. Alouini. On the secrecy capacity of MISO visible light communication channels. In *Proc. IEEE Globecom*, December 2016.

[9] M. A. Arfaoui, Z. Rezki, A. Ghrayeb, and M. S. Alouini. On the input distribution and optimal beamforming for the MISO VLC wiretap channel. In *Proc. IEEE GlobalSIP*, December 2016.

[10] G. Pan, J. Ye, and Z. Ding. On secure vlc systems with spatially random terminals. *IEEE Commun. Lett.*, 21(3):492–495, March 2017.

[11] M. A. Arfaoui, Z. Rezki, A. Ghrayeb, and M. S. Alouini. Discrete input signaling for MISO visible light communication channels. In *Proc. IEEE WCNC*, March 2017.

[12] S. Cho, G. Chen, and J. P. Coon. Secrecy analysis in visible light communication systems with randomly located eavesdroppers. In *Proc. IEEE ICC*, May 2017.

[13] 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. IWCMC*, June 2017.

[14] M. A. Arfaoui, A. Ghrayeb, and C. Assi. On the achievable secrecy rate of the MIMO VLC Gaussian wiretap channel. In *Proc. IEEE PIMRC*, October 2017.

[15] G. Pan, J. Ye, and Z. Ding. Secure hybrid VLC-RF systems with light energy harvesting. *IEEE Trans. Commun.*, 65(10):4348–4359, October 2017.

[16] L. Yin and H. Haas. Physical-layer security in multiuser visible light communication networks. *IEEE J. Sel. Areas Commun.*, 36(1):162–174, January 2018.

[17] S. Cho, G. Chen, and J. P. Coon. Physical layer security in visible light communication systems with randomly located colluding eavesdroppers. *IEEE Wireless Commun. Lett.*, 2018. To appear.

[18] M. A. Arfaoui, A. Ghrayeb, and C. Assi. Secrecy rate closed-form expressions for the SISO VLC wiretap channel with discrete input signaling. *IEEE Commun. Lett.*, 22(7):1382–1385, July 2018.

[19] T. V. Pham and A. T. Pham. On the secrecy sum-rate of MU-VLC broadcast systems with confidential messages. In *Proc. IEEE CSNDSP*, July 2016.

[20] M. A. Arfaoui, A. Ghrayeb, and C. Assi. Achievable secrecy sum-rate of the MISO VLC broadcast channel with confidential messages. In *Proc. IEEE Globecom*, December 2017.

[21] R. C. Kzilirimak, O. Narmanlioglu, and M. Uysal. Relay-assisted ofdm-based visible light communications. *IEEE Trans. Commun.*, 63(10):3765–3778, October 2015.

[22] T. Cover and J. A. Thomas. *Elements of Information Theory*. John Wiley & Sons, 2006.

[23] A. Arafa, E. Panayirci, and H. V. Poor. Relay-aided secure broadcasting for visible light communications. Available Online: arXiv:1809.03479.

[24] E. Ekrem and S. Ulukus. The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel. *IEEE Trans. Inf. Theory*, 57(4):2083–2114, April 2011.

[25] A. El Gamal and Y. H. Kim. *Network Information Theory*. Cambridge University Press, 2011.

[26] D. Tse and P. Viswanath. *Fundamentals of Wireless Communication*. Cambridge University Press, 2005.

[27] W. Dinkelbach. On nonlinear fractional programming. *Management Science*, 13(7):492–498, 1967.

[28] M. Uysal, C. Capsoni, Z. Ghassemlooy, A. Boucouvalas, and E. Udvary. *Optical Wireless Communications: An Emerging Technology*. Springer, 2016.