Relay-Aided Secure Broadcasting for Visible Light Communications

Ahmed Arafa, *Member, IEEE*, Erdal Panayirci, *Life Fellow, IEEE*, and H. Vincent Poor, *Fellow, IEEE*

***Abstract*— A visible light communication broadcast channel is considered, in which a transmitter luminaire communicates with two legitimate receivers in the presence of an external eavesdropper. A number of trusted *cooperative* half-duplex relay luminaires are deployed to aid with securing the transmitted data. Transmitters are equipped with single light fixtures, containing multiple light emitting diodes, and receiving nodes are equipped with single photo-detectors, rendering the considered setting as a single-input single-output system. Transmission is amplitude-constrained to maintain operation within the light emitting diodes' 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 multiple relaying schemes: *cooperative jamming*, *decode-and-forward*, and *amplify-and-forward*. Superposition coding with uniform signaling is used at the transmitter and the relays. Further, for each relaying scheme, *secure beamforming* vectors are carefully designed at the relay nodes in order to hurt the eavesdropper and/or benefit the legitimate receivers. Superiority of the proposed relaying schemes, with secure beamforming, is shown over direct transmission. It is also shown that the best relaying scheme depends on how far the eavesdropper is located from the transmitter and the relays, the number of relays, and their geometric layout.**

***Index Terms*— Visible light communication, LiFi, physical layer security, relays, cooperative jamming, decode-and-forward, amplify-and-forward, amplitude constraint.**

I. Introduction

VISIBLE light communications (VLC) technology is a promising candidate for future high-speed indoor communication systems, offering solutions to spectrum congestion issues in conventional radio frequency (RF) systems [2], [3]. 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 for wireless systems through jointly encoding for reliability and security, see, e.g., [4]. 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., [5]–[23]. The idea of employing an external friendly node that transmits jamming signals to degrade the eavesdropper channel is investigated in [5] and [6], under amplitude constraints that are imposed such that the light emitting diodes (LEDs) operate within their dynamic range, with [5] focusing on uniform signaling and [6] focusing on truncated Gaussian signaling. Achievable secrecy rates for the multiple-input single-output (MISO) VLC channel are derived in [7], which are then used for transmit beamforming signal design for the MISO setting in [8]. References [9], [10] also derive achievable secrecy rates for the MISO VLC channel and design transmit beamforming signals, yet with a focus on truncated generalized normal signaling, showing improvement over rates achieved by both uniform and truncated Gaussian signaling. Further improvements are later shown in [11] by using discrete signaling with finite number of mass points. Discrete signaling is also considered in [12], in which closed-form achievable secrecy rates for single-input single-output (SISO) VLC channels are derived. Reference [13] considers a multiple-input multiple-output (MIMO) VLC channel and derives achievable secrecy rates via designing transmit covariance matrices for uncorrelated symmetric logarithmic-concave input distributions. Secrecy outage probabilities are derived in [14]–[16] with multiple eavesdroppers, via tools from stochastic geometry and spatial point processes. Security aspects of hybrid VLC/RF setups are considered in [17] and [18]. A multiple-transmitter and multiple-eavesdropper scenario with one legitimate user is considered in [19], in which secrecy outage probabilities and ergodic secrecy rates with and without transmitters' cooperation are derived. Beamforming design techniques are proposed in [20] to provide security in cases where the locations of eavesdroppers are only statistically known. The impacts of how multipath light reflections can jeopardize security is studied in [21]. References [22], [23] are the most closely related to our work, in which broadcast VLC channels with confidential messages are considered and achievable secrecy sum rates are derived.

Motivated by their ability to improve the signal-to-noise ratio (SNR) and overall performance of optical wireless communication systems, relaying luminaires have been studied in [24]–[31] under various settings and assumptions,

Manuscript received September 7, 2018; revised January 11, 2019; accepted February 9, 2019. Date of publication February 22, 2019; date of current version June 14, 2019. This research was supported in part by the U.S. National Science Foundation under Grant CCF-093970 and Grant CCF-1513915. Erdal Panayirci has been supported by the Turkish Scientific and Research Council (TUBITAK) under the 1003 Primary Subjects R&D Funding Program, and in part by KAUST under Grant No. OSR-2016-CRG5-2958-02. This paper was presented in part at the IEEE Global Conference on Signal and Information Processing, Anaheim, CA, USA, November, 2018 [1]. The associate editor coordinating the review of this paper and approving it for publication was W. Xu. *(Corresponding author: Ahmed Arafa.)*

A. Arafa and H. V. Poor are with the Electrical Engineering Department, Princeton University, Princeton, NJ 08544 USA (e-mail: aarafa@princeton.edu; poor@princeton.edu).

E. Panayirci is with the Department of Electrical and Electronics Engineering, Kadir Has University, 34083 Istanbul, Turkey (e-mail: eepanay@khas.edu.tr).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TCOMM.2019.2900632

yet with no external eavesdroppers. Reference [24] studies amplify-and-forward and decode-and-forward relaying schemes, and shows that multi-hop diversity gains can be provided at the destination. Both relaying schemes are also studied in [25] to enhance achievable rates of mobile users. References [26], [27] consider multiple relaying scenarios where ceiling lights arranged in linear and triangular topologies help each other through multi-hop transmission. Several multiple relay-assisted VLC systems are proposed in [28], where it is shown that multi gigabit-per-second rates can be realized with simple optical modulation formats. In [29], an LED light bulb in a desk lamp is used as a relay for an OFDM-based VLC system. In [30], a cooperative VLC system is investigated in which an intermediate light source acts as a relay terminal operating in full duplex mode. Outage probability analysis is carried out in [31] under different relaying schemes in a hybrid VLC/RF setup.

Inspired by the above works, in this paper we investigate the role of using extra luminary sources acting as trusted *cooperative* half-duplex relays in securing a two-user broadcast VLC channel from an external eavesdropper. In our setting, an amplitude constraint is imposed upon the transmitted signal in order for the LEDs to operate within their dynamic range. Under such amplitude constraint, we first derive an achievable secrecy rate region, without using the relays, based on superposition coding with uniform signaling at the source. We then invoke the relays, and derive achievable secrecy rate regions for several relaying schemes: *cooperative jamming*, *decode-and-forward*, and *amplify-and-forward*, in all of which an amplitude constraint also applies to the relays' transmissions. For each relaying scheme, we design *secure beamforming* signals to maximize the achievable rates under the relays' amplitude constraints. The design of the beamforming signals is based on formulating optimization problems that are inferred from the derived achievable secrecy rates. Results show the enhancement, in general, of the achievable secrecy rates using the relays, and that the best relaying scheme highly depends on the eavesdropper's distance from the transmitter and the relays, and also on the number of relays and how they are geometrically laid out.

We note that while the methodologies involved in this work have been previously introduced for RF communications, there exists some differences that need to be carefully considered when employing them in the context of VLC. First, and as mentioned above, a physical amplitude constraint applies to all transmitted signals from the LEDs. Invoking amplitude constraints calls for new transmission signaling design. For instance, Gaussian signaling, which is optimal for additive white Gaussian noise channels with *average* power constraints, is not even feasible here. We work with uniform signaling, as done in some works in the VLC literature, e.g., [5], [7], [8], and derive achievable secrecy rate regions based on superposition coding using information-theoretic tools. To the best of our knowledge, this is the first time that achievable information-theoretic secrecy rate regions are derived under amplitude constraints for multiuser VLC with cooperative relays. Our analysis yields closed-form expressions that enable optimal design of the relay beamforming signals using linear-algebraic and optimization tools, which are shown to boost the achievable secrecy rate regions in general. Second, the VLC channel model is also different from conventional RF channel models; the indoor line-of-sight model used is largely deterministic, and strongly related to the Euclidean distance of the transmission link. The channel gain is real-valued, positive, and depends mainly on the relative locations between the nodes, in addition to some physical characteristics of the illuminating LEDs.

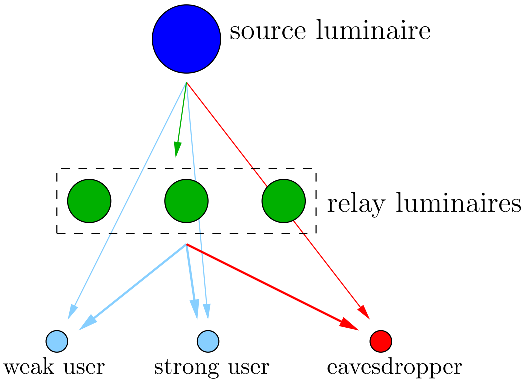


Fig. 1. An indoor VLC system model in which a source luminaire communicates with two legitimate users in the presence of an eavesdropper. A number of cooperative trusted relaying luminaires assist with the source's transmission.

It is worth mentioning that sending information simultaneously to multiple users over the same resource block using superposition coding is commonly referred to, in the recent wireless communications literature, as non-orthogonal multiple access (NOMA) [32], [33]. Our approach can then be viewed as providing security at the physical layer using cooperative relays in a VLC channel in which NOMA techniques are employed.

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 electric 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 electric 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 employs superposition coding [34] 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 VLC, since the signal is modulated onto the intensity of the emitted light, it must satisfy amplitude (or equivalently *peak*

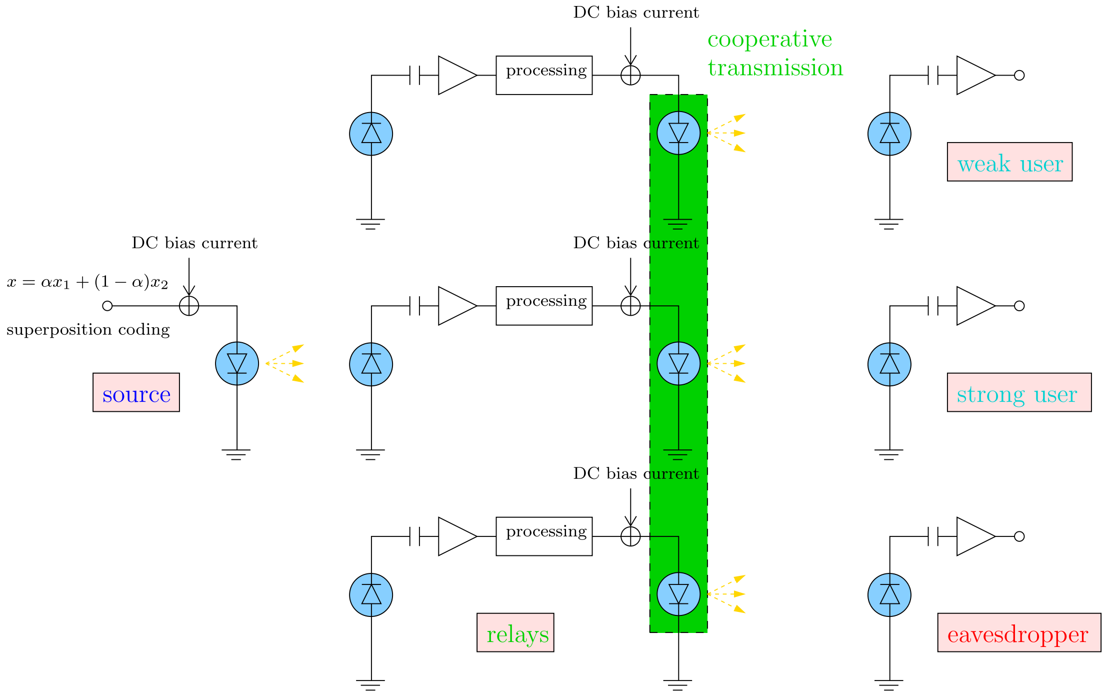


Fig. 2. A schematic diagram illustrating the considered VLC system model.

power) constraints that are imposed by the dynamic range of typical LEDs to maintain linear current-light conversion and avoid clipping distortion. An amplitude constraint, $A > 0$, is enforced as follows:

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

The VLC channel gain between the transmitting LEDs of a light fixture and a PD is given by [35]

$$\frac{A_{det}(m+1)}{2\pi l^2}\left(\frac{|z_{diff}|}{l}\right)^{m+1}, \tag{3}$$

where A_{det} ie the PD's physical area in squared meters, $m = -\log(2)/\log\left(\cos\phi_{\frac{1}{2}}\right)$ is the order of Lambertian emission,[1] with $\phi_{\frac{1}{2}}$ denoting the LED semi-angle at half power, l denoting the distance between the LEDs and the PD, and z_{diff} denoting the vertical distance between them. Note the VLC channel gain in the above model is positive and real-valued.

Let h_1, h_2, and h_e denote the channel gains between the source and the first user, the second user, and the eavesdropper, respectively. Without loss of generality, let $h_1 > h_2$, and hence the first user decodes the second user's message first then uses successive interference cancellation to decode its own message, while the second user decodes its message by treating the first user's interfering signal as noise [34]. From this point on, we denote the first user and the second user as the *strong* user and the *weak* user, respectively. We denote by y_1, y_2, and y_e the received signals, in the electric domain, at the strong user, the weak user, and the eavesdropper, respectively. These are

$$y_1 = h_1 x + n_1, \tag{4}$$

$$y_2 = h_2 x + n_2, \tag{5}$$

$$y_e = h_e x + n_e, \tag{6}$$

where n_1, n_2, and n_e are i.i.d. $\sim \mathcal{N}(0,1)$ noise terms.[2]

A number of extra luminary sources acting as *trusted cooperative* half duplex relay nodes are available to aid with securing data from the eavesdropper. Such relay nodes can be, e.g., mounted on the walls of the room in between the source and the users, or hanging from the ceiling in between them, which is possibly deployable in buildings with multi-layered lighting structures, see Fig. 1 and the schematic diagram in Fig. 2. Let there be K relays, and denote the channel gains from the source to the relays by the vector[3] $\mathbf{h}_r \triangleq [h_{r,1}, \ldots, h_{r,K}]$. Let $\mathbf{g}_1$, $\mathbf{g}_2$, and $\mathbf{g}_e$ denote the K-length channel gain vectors from the relays to the strong user, the weak user, and the eavesdropper, respectively. All channel gains: h_j, $j = 1, 2, e$, $\mathbf{h}_r$ and $\mathbf{g}_j$, $j = 1, 2, e$, are assumed to be known at the source. On the other hand, the channel gains $\mathbf{g}_j$, $j = 1, 2, e$, are assumed to be known at the relays.

Similar to the source, we assume an amplitude constraint, $\bar{A} > 0$, applies to the relays' transmitted signal. In order to have a fair comparison between the relaying and non-relaying scenarios, we set $\bar{A} = \gamma A$ for some fraction $\gamma \in [0,1]$ to be designed. Operationally, we interpret the amplitude constraint as a *peak* power constraint at the LEDs. Hence, in case of relaying, the effective amplitude constraint that applies at the source's LEDs reduces to $A_\gamma \triangleq \sqrt{1-\gamma^2}A$. The fraction γ^2 therefore divides the total system's peak power budget A^2

[1] log terms in this paper denote natural logarithms.

[2] We choose to normalize the noise variances in this paper for simplicity of presentation, and take that effect on the SNR into the amplitude constraint's value. That is, the SNR is now given by the square of the channel gain multiplied by the square of the amplitude constraint.

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

among the source and the relays. This condition is to serve the purpose of avoiding situations in which one can add relaying LEDs at no extra cost.

In the following sections, we derive achievable secrecy rates when the source and the relays transmit their data using uniform signaling schemes. We first compute the rates without using the relays, i.e., with $\gamma = 0$, and then compare them to the rates achieved under various relaying strategies: *cooperative jamming*, *decode-and-forward*, and *amplify-and-forward*. For these relaying schemes, we state the results for general $\gamma \in [0, 1]$, and then discuss the optimal design of γ in Section VII.

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 the following theorem, whose proof is in Appendix A:

Theorem 1: *The following secrecy rate pair, for the strong and weak users, is achievable via direct transmission for a given α:*

$$r_{1,s} = \left[\frac{1}{2}\log\left(1+\frac{2h_1^2\alpha^2A^2}{\pi e}\right)-\frac{1}{2}\log\left(1+\frac{h_e^2\alpha^2A^2}{3}\right)\right]^+, \quad (7)$$

$$r_{2,s} = \left[\frac{1}{2}\log\left(\frac{1+\frac{2h_2^2A^2}{\pi e}}{1+\frac{h_2^2\alpha^2A^2}{3}}\right)-\frac{1}{2}\log\left(\frac{1+\frac{h_e^2A^2}{3}}{1+\frac{2h_e^2\alpha^2A^2}{\pi e}}\right)\right]^+, \quad (8)$$

where the second subscript s is to denote secrecy rates, and $[\cdot]^+ \triangleq \max(\cdot, 0)$.

Observe that for $\alpha = 1$, we obtain $r_{2,s} = 0$ since $\frac{2}{\pi e} < \frac{1}{3}$, and $r_{1,s}$ coincides with the SISO achievable secrecy rate derived in [7], since the signal now is only directed toward one user (the strong user). The opposite holds for $\alpha = 0$ as well. It is also clear from (7) and (8) that the strong user's achievable secrecy rate is positive if and only if (iff)

$$\frac{2}{\pi e}h_1^2 > \frac{1}{3}h_e^2, \quad (9)$$

and that the weak user's achievable secrecy rate is positive iff

$$\left(\frac{2}{\pi e}-\frac{\alpha^2}{3}\right)h_2^2+\left(\frac{2\alpha^2}{\pi e}-\frac{1}{3}\right)h_e^2 > \left(\frac{1}{9}-\frac{4}{\pi^2e^2}\right)\alpha^2h_2^2h_e^2. \quad (10)$$

Thus, achieving positive secrecy rates depends on the relative channel conditions between the users and the eavesdropper as articulated by the above inequalities. In the following sections, we study how to enhance the achievable secrecy rates in Theorem 1 above by using cooperative trusted relays.

IV. Cooperative Jamming

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

$$|z| \leq \bar{A} \quad \text{a.s.}, \quad (11)$$

$$\|\mathbf{J}\|_1 \leq 1, \quad (12)$$

where $\|\cdot\|_1$ denotes the L_1 norm operator: $\|\mathbf{J}\|_1 = \sum_{i=1}^K |J_i|$. Observe that applying an L_1 norm constraint has the operational meaning that the cooperative relaying LEDs share the peak power budget $\bar{A}^2 = \gamma^2A^2$ allocated to them, whereas if an L_∞ norm is used instead, i.e., if we set: $\max_i |J_i| \leq 1$, then this would mean that each relay comes with its own power budget independently, i.e., the peak power budget $\bar{A}^2 = \gamma^2A^2$ would be given to *each* relay, which would not be fair to compare with the non-relaying scenario. The received signals at the legitimate users and the eavesdropper are now given by

$$y_1 = h_1x + \mathbf{g}_1^T\mathbf{J}z + n_1, \quad (13)$$

$$y_2 = h_2x + \mathbf{g}_2^T\mathbf{J}z + n_2, \quad (14)$$

$$y_e = h_ex + \mathbf{g}_e^T\mathbf{J}z + n_e, \quad (15)$$

where the superscript T denotes the transpose operation, and the amplitude constraint on the transmitted signal x is now reduced to $A_\gamma = \sqrt{1-\gamma^2}A$.

In order not to harm the legitimate users, the beamforming vector is designed such that

$$\mathbf{g}_1^T\mathbf{J} = \mathbf{g}_2^T\mathbf{J} = 0, \quad (16)$$

which is guaranteed if $K \geq 3$ relays, making the matrix $\mathbf{G}^T \triangleq [\mathbf{g}_1 \ \mathbf{g}_2]^T$ have a non-empty null space. Let us denote the beamforming vector satisfying (16) by $\mathbf{J}_o$. We now have the following result, whose proof is in Appendix B:

Theorem 2: *The following secrecy rate pair, for the strong and weak users, is achievable via cooperative jamming for a given α:*

$$r_{1,s}^J = \left[\frac{1}{2}\log\left(1+\frac{2h_1^2\alpha^2A_\gamma^2}{\pi e}\right)\right.$$
$$\left.-\frac{1}{2}\log\left(\frac{1+\frac{h_e^2\alpha^2A_\gamma^2}{3}+\frac{\left(\mathbf{g}_e^T\mathbf{J}_o\right)^2\bar{A}^2}{3}}{1+\frac{2(\mathbf{g}_e^T\mathbf{J}_o)^2\bar{A}^2}{\pi e}}\right)\right]^+, \quad (17)$$

$$r_{2,s}^J = \left[\frac{1}{2}\log\left(\frac{1+\frac{2h_2^2A_\gamma^2}{\pi e}}{1+\frac{h_2^2\alpha^2A_\gamma^2}{3}}\right)\right.$$
$$\left.-\frac{1}{2}\log\left(\frac{1+\frac{h_e^2A_\gamma^2}{3}+\frac{\left(\mathbf{g}_e^T\mathbf{J}_o\right)^2\bar{A}^2}{3}}{1+\frac{2h_e^2\alpha^2A_\gamma^2}{\pi e}+\frac{2(\mathbf{g}_e^T\mathbf{J}_o)^2\bar{A}^2}{\pi e}}\right)\right]^+, \quad (18)$$

where the superscript J is to denote the cooperative jamming scheme.

We now proceed to find the optimal beamforming vector $\mathbf{J}_o$ that maximally degrades the eavesdropper's channel. In view of (17) and (18), by direct first derivative analysis, one can show that $r_{1,s}^J$ is increasing in $\left(\mathbf{g}_e^T\mathbf{J}_o\right)^2$ iff

$$h_e^2\alpha^2A_\gamma^2 > \frac{\pi e}{2} - 3 \approx 1.27, \quad (19)$$

and that $r_{2,s}^J$ is increasing in $\left(\mathbf{g}_e^T\mathbf{J}_o\right)^2$ iff

$$h_e^2\left(1-\alpha^2\right)A_\gamma^2 > \frac{\pi e}{2} - 3 \approx 1.27. \quad (20)$$

We note that, as a direct consequence of the data processing inequality [34], sending a jamming signal can only degrade the eavesdropper's channel. It is clear, however, that the inequalities in (19) and (20) 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 lower bounds on the achievable secrecy rates, as opposed to exact computations. Whenever the secrecy rate (of either user) is increasing in $\left(\mathbf{g}_e^T\mathbf{J}_o\right)^2$, we find the optimal beamforming vector $\mathbf{J}_o^*$ by solving the following optimization problem:

$$\begin{aligned} \max_{\mathbf{J}_o} \quad & \left(\mathbf{g}_e^T\mathbf{J}_o\right)^2 \\ \text{s.t.} \quad & \mathbf{G}^T\mathbf{J}_o = \left[0\ 0\right] \\ & \|\mathbf{J}_o\|_1 \leq 1. \end{aligned} \tag{21}$$

To solve the above problem, we first introduce the following orthogonal projection notation onto the null space of $\mathbf{G}^T$:

$$\mathcal{P}^{\perp}(\mathbf{G}) \triangleq \mathbf{I}_K - \mathbf{G}\left(\mathbf{G}^T\mathbf{G}\right)^{-1}\mathbf{G}^T, \tag{22}$$

where $\mathbf{I}_K$ denotes the $K \times K$ identity matrix.[4] It is clear that any vector lying in the null space of $\mathbf{G}^T$ can be written as the multiplication of $\mathcal{P}^{\perp}(\mathbf{G})$ by some vector $\mathbf{u}_J \in \mathbb{R}^K$. The optimal $\mathbf{J}_o^*$ vector should then be of the form

$$\mathbf{J}_o^* = \mathcal{P}^{\perp}(\mathbf{G})\,\mathbf{u}_J, \tag{23}$$

whence the objective function of problem (21) would be given by $\left(\mathbf{g}_e^T\mathcal{P}^{\perp}(\mathbf{G})\,\mathbf{u}_J\right)^2$, which is maximized by choosing $\mathbf{u}_J = c_J\mathcal{P}^{\perp}(\mathbf{G})\,\mathbf{g}_e$, for some constant $c_J \in \mathbb{R}$. Finally, to satisfy the amplitude constraint, we choose the constant c_J such that

$$\mathbf{J}_o^* = \frac{\mathcal{P}^{\perp}(\mathbf{G})\,\mathbf{g}_e}{\|\mathcal{P}^{\perp}(\mathbf{G})\,\mathbf{g}_e\|_1}. \tag{24}$$

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

$$\mathbf{y}_r = \mathbf{h}_r x + \mathbf{n}_r, \tag{25}$$

where $\mathbf{n}_r \sim \mathcal{N}(\mathbf{0}, \mathbf{I}_K)$ represents the Gaussian noise in the source-relays channels. In the second phase, the ith relay decodes its received signal to find x_1 and x_2, re-encodes x_1 into $\tilde{x}_1$ and x_2 into $\tilde{x}_2$ using independent codewords, and then forwards them to the users using superposition coding after multiplying its transmitted signal by a constant $d_i \in \mathbb{R}$ to be designed. Effectively, the relays' transmitted signal in the second phase is given by $\mathbf{d}x_r$, with $\mathbf{d} = [d_1, d_2, \ldots, d_K]$, and x_r given by

$$x_r = \alpha\tilde{x}_1 + (1-\alpha)\tilde{x}_2. \tag{26}$$

That is, we assume the relays use the same α fraction as the source. The following constraints hold at the relays:

$$\alpha|\tilde{x}_1| + (1-\alpha)|\tilde{x}_2| \leq \bar{A} \quad \text{a.s.,} \tag{27}$$

$$\|\mathbf{d}\|_1 \leq 1. \tag{28}$$

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

$$y_1^r = \mathbf{g}_1^T\mathbf{d}x_r + n_1^r, \tag{29}$$

$$y_2^r = \mathbf{g}_2^T\mathbf{d}x_r + n_2^r, \tag{30}$$

$$y_e^r = \mathbf{g}_e^T\mathbf{d}x_r + n_e^r, \tag{31}$$

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

For the number of relays $K \geq 2$, we propose designing the beamforming vector $\mathbf{d}$ to satisfy

$$\mathbf{g}_e^T\mathbf{d} = 0 \tag{32}$$

so that the eavesdropper does not receive any useful information in the second phase. We denote such beamforming signal by $\mathbf{d}_o$. If $K \geq 3$, then it will hold that both $\mathbf{g}_1^T\mathbf{d}_o$ and $\mathbf{g}_2^T\mathbf{d}_o$ are non-zero a.s. We now have the following theorem, whose proof is in Appendix C:

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

$$r_{1,s}^{DF} = \frac{1}{2}\left[r_1^{DF} - \frac{1}{2}\log\left(1 + \frac{h_e^2\alpha^2A_\gamma^2}{3}\right)\right]^+, \tag{33}$$

$$r_{2,s}^{DF} = \frac{1}{2}\left[r_2^{DF} - \frac{1}{2}\log\left(\frac{1 + \frac{h_e^2A_\gamma^2}{3}}{1 + \frac{2h_e^2\alpha^2A_\gamma^2}{\pi e}}\right)\right]^+, \tag{34}$$

where the superscript DF is to denote the decode-and-forward scheme, and r_1^{DF} and r_2^{DF} given by (35) and (36), respectively, at the top of the next page.

In view of (35) and (36), we see that r_1^{DF} is increasing in $\left(\mathbf{g}_1^T\mathbf{d}_o\right)^2$, while direct first derivative analysis shows that r_2^{DF} is increasing in $\left(\mathbf{g}_1^T\mathbf{d}_o\right)^2$ 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:

$$\begin{aligned} \max_{\mathbf{d}_o} \quad & \alpha\left(\mathbf{g}_1^T\mathbf{d}_o\right)^2 + (1-\alpha)\left(\mathbf{g}_2^T\mathbf{d}_o\right)^2 \\ \text{s.t.} \quad & \mathbf{g}_e^T\mathbf{d}_o = 0 \\ & \|\mathbf{d}\|_1 \leq 1. \end{aligned} \tag{37}$$

To satisfy the first constraint, the optimal $\mathbf{d}_o^*$ should be of the form

$$\mathbf{d}_o^* = \mathcal{P}^{\perp}(\mathbf{g}_e)\,\mathbf{u}_d \triangleq \mathbf{F}_d\mathbf{u}_d \tag{38}$$

for some vector $\mathbf{u}_d \in \mathbb{R}^K$ to be designed, with $\mathcal{P}^{\perp}(\cdot)$ as defined in (22). To choose the best $\mathbf{u}_d$, we rewrite the objective function of the above problem slightly differently as follows:

$$\mathbf{u}_d^T\mathbf{F}_d\left(\alpha\mathbf{g}_1\mathbf{g}_1^T + (1-\alpha)\mathbf{g}_2\mathbf{g}_2^T\right)\mathbf{F}_d\mathbf{u}_d. \tag{39}$$

Therefore, the optimal $\mathbf{u}_d$ is given by

$$\mathbf{u}_d = c_d\mathbf{v}_d, \tag{40}$$

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

$$r_1^{DF}=\min\left\{\frac{1}{2}\log\left(1+\frac{2h_1^2\alpha^2A_\gamma^2}{\pi e}\right)+\frac{1}{2}\log\left(1+\frac{2\left(\mathbf{g}_1^T\mathbf{d}_o\right)^2\alpha^2\bar{A}^2}{\pi e}\right),\frac{1}{2}\log\left(1+\min_{1\le i\le K}\frac{2h_{r,i}^2\alpha^2A_\gamma^2}{\pi e}\right)\right\} \quad (35)$$

$$r_2^{DF}=\min\left\{\frac{1}{2}\log\left(\frac{1+\frac{2h_2^2A_\gamma^2}{\pi e}}{1+\frac{h_2^2\alpha^2A_\gamma^2}{3}}\right)+\frac{1}{2}\log\left(\frac{1+\frac{2\left(\mathbf{g}_2^T\mathbf{d}_o\right)^2\bar{A}^2}{\pi e}}{1+\frac{\left(\mathbf{g}_2^T\mathbf{d}_o\right)^2\alpha^2\bar{A}^2}{3}}\right),\frac{1}{2}\log\left(\min_{1\le i\le K}\frac{1+\frac{2h_{r,i}^2A_\gamma^2}{\pi e}}{1+\frac{h_{r,i}^2\alpha^2A_\gamma^2}{3}}\right)\right\} \quad (36)$$

where $c_d\in\mathbb{R}$ is a constant, and $\mathbf{v}_d$ is the leading eigenvector of the matrix

$$\mathbf{F}_d\left(\alpha\mathbf{g}_1\mathbf{g}_1^T+(1-\alpha)\mathbf{g}_2\mathbf{g}_2^T\right)\mathbf{F}_d, \quad (41)$$

i.e., the eigenvector corresponding to the largest eigenvalue of the matrix. Finally, we choose c_d to satisfy the amplitude constraint as follows:

$$\mathbf{u}_d=\frac{\mathbf{v}_d}{\|\mathbf{v}_d\|_1}. \quad (42)$$

VI. Amplify-and-Forward

In this section, we discuss the amplify-and-forward scheme. As in the decode-and-forward scheme, communication occurs over two phases. However, in the second phase, 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 $\texttt{diag}\left(\mathbf{y}_r\right)\mathbf{a}$, where $\texttt{diag}(\mathbf{l})$ is the diagonalization of the vector $\mathbf{l}$, and the following amplitude constraint holds at the relays:

$$\left\|\texttt{diag}\left(\mathbf{y}_r\right)\mathbf{a}\right\|_1\le\bar{A}\quad\text{a.s.} \quad (43)$$

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

$$y_1^r=\mathbf{g}_1^T\texttt{diag}\left(\mathbf{y}_r\right)\mathbf{a}+n_1^r, \quad (44)$$
$$y_2^r=\mathbf{g}_2^T\texttt{diag}\left(\mathbf{y}_r\right)\mathbf{a}+n_2^r, \quad (45)$$
$$y_e^r=\mathbf{g}_e^T\texttt{diag}\left(\mathbf{y}_r\right)\mathbf{a}+n_e^r. \quad (46)$$

As in the decode-and-forward scheme, for $K\ge2$ relays, we propose designing the beamforming vector $\mathbf{a}$ to satisfy

$$\mathbf{g}_e^T\texttt{diag}\left(\mathbf{h}_r\right)\mathbf{a}=0 \quad (47)$$

so that the eavesdropper does not receive any useful information in the second phase. We denote such beamforming signal by $\mathbf{a}_o$. Further, for $K\ge3$ relays, it holds that both $\mathbf{g}_1^T\texttt{diag}\left(\mathbf{h}_r\right)\mathbf{a}_o$ and $\mathbf{g}_2^T\texttt{diag}\left(\mathbf{h}_r\right)\mathbf{a}_o$ are non-zero a.s. We now have the following theorem, whose proof is in Appendix D:

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

$$r_{1,s}^{AF}=\frac{1}{2}\left[\frac{1}{2}\log\left(1+\frac{2\kappa_1^2\alpha^2A_\gamma^2}{\pi e}\right)-\frac{1}{2}\log\left(1+\frac{h_e^2\alpha^2A_\gamma^2}{3}\right)\right]^+, \quad (48)$$

$$r_{2,s}^{AF}=\frac{1}{2}\left[\frac{1}{2}\log\left(\frac{1+\frac{2\kappa_2^2A_\gamma^2}{\pi e}}{1+\frac{\kappa_2^2\alpha^2A_\gamma^2}{3}}\right)-\frac{1}{2}\log\left(\frac{1+\frac{h_e^2A_\gamma^2}{3}}{1+\frac{2h_e^2\alpha^2A_\gamma^2}{\pi e}}\right)\right]^+, \quad (49)$$

where the superscript AF is to denote the amplify-and-froward scheme, and

$$\kappa_j^2\triangleq h_j^2+\frac{\left(\mathbf{g}_j^T\texttt{diag}\left(\mathbf{h}_r\right)\mathbf{a}_o\right)^2}{1+\left(\mathbf{g}_j^T\mathbf{a}_o\right)^2},\quad j=1,2. \quad (50)$$

In view of (48) and (49), 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 $\alpha\le\sqrt{\frac{2/\pi e}{1/3}}\approx0.838$, yet again this condition can be ignored (as we did in the decode-and-forward case) since $r_{2,s}^{AF}$ can only be positive if $\alpha\le0.838$. Therefore, we propose the following fractional optimization problem to find the best beamforming vector that maximizes the jth user's rate, $j=1,2$:

$$\begin{aligned}\max_{\mathbf{a}_o}\quad&\frac{\left(\mathbf{g}_j^T\texttt{diag}\left(\mathbf{h}_r\right)\mathbf{a}_o\right)^2}{1+\left(\mathbf{g}_j^T\mathbf{a}_o\right)^2}\\ \text{s.t.}\quad&\mathbf{g}_e^T\texttt{diag}\left(\mathbf{h}_r\right)\mathbf{a}_o=0\\ &\left\|\texttt{diag}\left(\mathbf{y}_r\right)\mathbf{a}_o\right\|_1\le\bar{A}.\end{aligned} \quad (51)$$

To solve the above fractional program, we introduce the following auxiliary problem:

$$\begin{aligned}p_j^{AF}(\lambda)\triangleq\max_{\mathbf{a}_o}\quad&\left(\mathbf{g}_j^T\texttt{diag}\left(\mathbf{h}_r\right)\mathbf{a}_o\right)^2-\lambda\left(1+\left(\mathbf{g}_j^T\mathbf{a}_o\right)^2\right)\\ \text{s.t.}\quad&\mathbf{g}_e^T\texttt{diag}\left(\mathbf{h}_r\right)\mathbf{a}_o=0\\ &\left\|\texttt{diag}\left(\mathbf{y}_r\right)\mathbf{a}_o\right\|_1\le\bar{A}\end{aligned} \quad (52)$$

for some $\lambda\ge0$. One can show the following: 1) $p_j^{AF}(\lambda)$ is decreasing in λ; and 2) the optimal solution of problem (51) is given by λ^* that solves $p_j^{AF}\left(\lambda^*\right)=0$ [36]. Hence, one can find an upper bound on λ^* that makes $p_j^{AF}(\lambda)<0$ and then proceed by, e.g., a bisection search, to find λ^*. Focusing on problem (52), we first note that, to satisfy the first constraint, the optimal $\mathbf{a}_o$ should be of the form

$$\mathbf{a}_o=\mathcal{P}^\perp(\texttt{diag}\left(\mathbf{h}_r\right)\mathbf{g}_e)\,\mathbf{u}_a\triangleq\mathbf{F}_a\mathbf{u}_a \quad (53)$$

for some vector $\mathbf{u}_a\in\mathbb{R}^K$ to be designed. To choose the best $\mathbf{u}_a$, we rewrite the objective function as

$$\mathbf{u}_a^T\mathbf{F}_a\left(\texttt{diag}\left(\mathbf{h}_r\right)\mathbf{g}_j\mathbf{g}_j^T\texttt{diag}\left(\mathbf{h}_r\right)-\lambda\mathbf{g}_j\mathbf{g}_j^T\right)\mathbf{F}_a\mathbf{u}_a. \quad (54)$$

Hence, the optimal $\mathbf{u}_a$ is given by

$$\mathbf{u}_a=c_a\mathbf{v}_a, \quad (55)$$

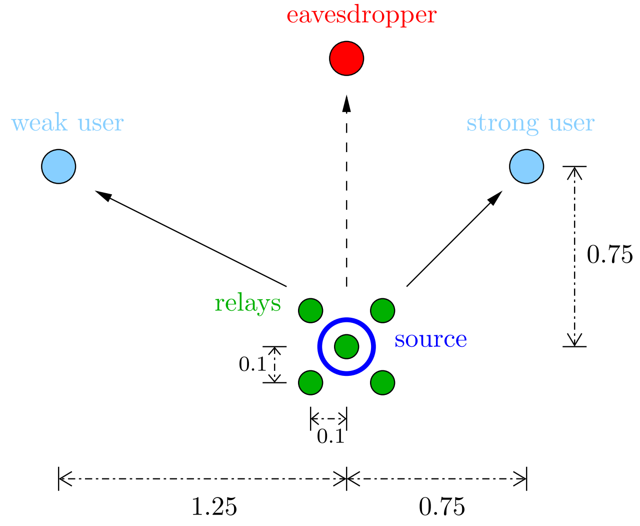


Fig. 3. Plan view of the geometric layout of the source, the relays, the legitimate users, and the eavesdropper.

where $c_a \in \mathbb{R}$ is a constant, and $\mathbf{v}_a$ is the leading eigenvector of the matrix

$$\mathbf{F}_a \left(\mathtt{diag}\left(\mathbf{h}_r\right)\mathbf{g}_j\mathbf{g}_j^T\mathtt{diag}\left(\mathbf{h}_r\right) - \lambda\mathbf{g}_j\mathbf{g}_j^T\right)\mathbf{F}_a. \tag{56}$$

We choose c_a to satisfy the amplitude constraint as follows:

$$\mathbf{u}_a = \frac{\mathbf{v}_a}{\left\|\mathtt{diag}\left(\mathbf{y}_r\right)\mathbf{v}_a\right\|_1}\bar{A}. \tag{57}$$

Finally, let $\mathbf{a}_o^{(j)}$ be the solution of problem (51). We propose using the following beamforming vector:

$$\mathbf{a}_o^* = \alpha\mathbf{a}_o^{(1)} + (1-\alpha)\mathbf{a}_o^{(2)}. \tag{58}$$

VII. Numerical Evaluations and Discussion

In this section, we validate our results via numerical evaluations and discuss the relative performances of the proposed schemes in this paper. We characterize the boundary of the achievable secrecy regions of the different schemes by solving the following optimization problem for a given $\mu \in [0,1]$:

$$\begin{aligned} \max_{\alpha,\gamma} \quad & \mu r_{1,s}^{\omega} + (1-\mu)r_{2,s}^{\omega} \\ \text{s.t.} \quad & 0 \le \alpha \le 1, \quad 0 \le \gamma \le 1, \end{aligned} \tag{59}$$

with $\omega \in \{J, DF, AF\}$ denoting the relaying scheme, or is simply not used in the case of direct transmission. We solve the above problem numerically using, e.g., a line search algorithm. Since the feasible set is bounded, this facilitates convergence to an optimal solution. For simplicity, we set $\lambda = 1$ in the AF beamforming vector optimization and do not further optimize it.

We consider a room of size $5 \times 5 \times 3$ cubic meters. With the origin tuple $(0,0,0)$ denoting the center of the room's floor. The source is located at $(0,0,3)$, the strong user at $(0.75, 0.75, 0.7)$, and the weak user at $(-1.25, 0.75, 0.7)$.

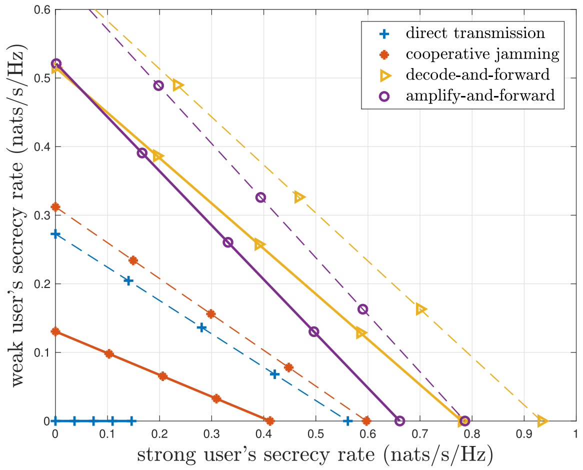


Fig. 4. Achievable secrecy regions of the proposed schemes. Solid lines are with eavesdropper at $(0, 1.5, 0.7)$, and dashed lines are with it at $(0, 2, 0.7)$.

We consider $K = 5$ relays located at the following positions: $(0.1, 0.1, 2)$, $(0.1, -0.1, 2)$, $(0, 0, 2)$, $(-0.1, 0.1, 2)$, and $(-0.1, -0.1, 2)$, see the plan view in Fig. 3. The channel gain between two nodes is given by (3), with $A_{det} = 10^{-4}$ and $\phi_{\frac{1}{2}} = 60°$. We set the amplitude constraint (or the system's peak power budget) to $A = 10^7$.

In Fig. 4, the achievable secrecy rate regions of the schemes proposed in this paper, along with that of the direct transmission scheme are shown. The solid lines in Fig. 4 are when the eavesdropper is located at $(0, 1.5, 0.7)$. We see in this case that all the proposed schemes perform strictly better than direct transmission. The dashed lines in Fig. 4 are when the eavesdropper is located a bit further away from the source (and the relays) at $(0, 2, 0.7)$. We see in this case that larger secrecy rates are achievable for all schemes, and that direct transmission is now comparable to cooperative jamming. We also note that they are both performing *closer* in this case to decode-and-forward and amplify-and-forward. The main reason behind this is that as the eavesdropper gets further away from the source, the *rate of increase* in the achievable secrecy rates in case of direct transmission and cooperative jamming becomes *larger* than that of decode-and-forward and amplify-and-forward. This is attributed to the extra pre-log $\frac{1}{2}$ terms in the case of decode-and-forward and amplify-and-forward that are due to the half-duplex operation of the relays. These terms have a diminishing effect on the achievable secrecy rates that becomes more apparent as the eavesdropper gets further away, whence direct transmission and cooperative jamming start performing better.

In Fig. 5, we investigate this latter note further, and show the effect of the eavesdropper's distance from the source on the secrecy sum rate, setting $\mu = \frac{1}{2}$ in problem (59). We vary the eavesdropper's location from $(0, 0.75, 0.7)$ to $(0, 4, 0.7)$, i.e., we only change its location's second coordinate's value. We observe from the figure that clearly the secrecy sum rate increases, for all schemes, as the eavesdropper's distance from the source increases. We also note that at relatively close locations, the proposed relaying schemes achieve strictly positive rates, as opposed to the zero rate achieved via direct

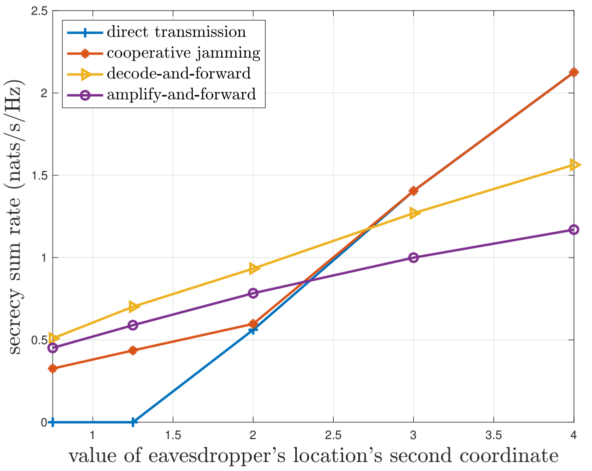


Fig. 5. Effect of eavesdropper's distance from the source on the achievable secrecy sum rate. Only the second coordinate of the eavesdropper's location is varied, while the first and the third coordinates are fixed at 0 and 0.7, respectively.

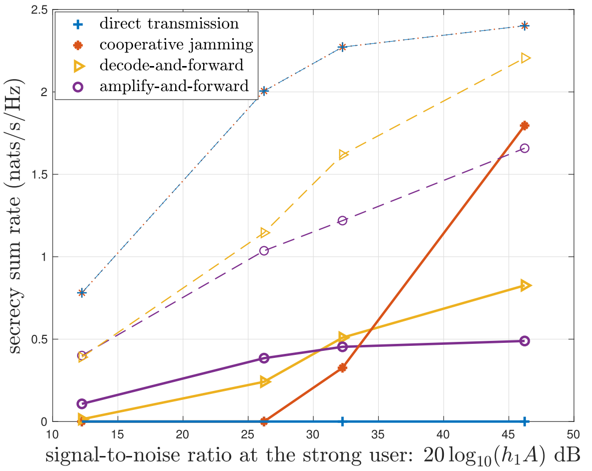


Fig. 6. Effect of the strong user's SNR on the achievable secrecy sum rate. Solid lines are with the eavesdropper at $(0, 0.75, 0.7)$, and dashed lines are with it at $(0, 4.25, 0.7)$.

transmission. This shows how useful the proposed relaying schemes become, compared to direct transmission, when the eavesdropper is relatively close to the source. Finally, it can be seen from the figure that there exists a certain distance after which direct transmission and cooperative jamming beat decode-and-forward and amplify-and-forward. This is attributed to, as discussed before, the diminishing effects of the extra pre-log $\frac{1}{2}$ terms in the case of decode-and-forward and amplify-and-forward, which are not present in direct transmission and cooperative jamming.

In Fig. 6, we show the effect of the SNR at the strong user on the achievable secrecy sum rates. The strong user's SNR (in dB) is given by $20\log_{10}(h_1 A)$. We consider a setting in which the eavesdropper is close-by at $(0, 0.75, 0.7)$, whose results are depicted in solid lines, and another setting in which the eavesdropper is far-away at $(0, 4.25, 0.7)$, whose results are depicted in dashed lines. In the close-by setting, direct transmission achieves zero rate for all values of the SNR, cooperative jamming starts achieving positive rates only for relatively higher values of the SNR and continues to eventually beat all other schemes, amplify-and-forward performs best at relatively lower SNR values and is beaten by decode-and-forward at relatively higher ones. In the far-away setting, direct transmission and cooperative jamming are indistinguishable, and beat decode-and-forward and amplify-and-forward for all values of the SNR. This is, once more, the effect of the half-duplex operation of the relays. It is clear from Figs. 4, 5, and 6 that the best relaying scheme depends on the secrecy rate region's operating point, the distance between the source and the eavesdropper and the SNR.

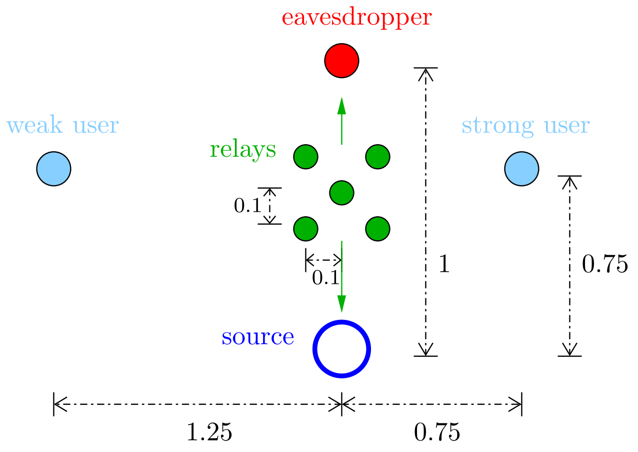


Fig. 7. Plan view of the geometric layout of the system, in which the center point of the relays' positions is varying.

Next, we explore another aspect of relative distances between the nodes by fixing the eavesdropper's location at $(0, 1, 0.7)$ and varying the centroid of the relays' positions. Specifically, we let the relays be located at $(0.1, c_y + 0.1, 2)$, $(0.1, c_y - 0.1, 2)$, $(0, c_y, 2)$, $(-0.1, c_y + 0.1, 2)$, and $(-0.1, c_y - 0.1, 2)$ and vary the center point c_y from -0.5 to 1.5, see the plan view in Fig. 7. We plot the achievable secrecy sum rates versus c_y in Fig. 8. We see from the figure that direct transmission achieves zero secrecy rates for all values of c_y, since the eavesdropper is relatively closer to the source than the legitimate users. On the other hand, all the proposed relaying schemes achieve strictly positive secrecy rates, with varying performances. We notice, in particular, that the relatively simple cooperative jamming scheme performs best when the relays are closest to the eavesdropper.

Finally, we explore the effect of a different aspect on the secrecy sum rate: the number of relay nodes, and how far apart they are from each other. We consider the situation in which the eavesdropper is located relatively close to the source at $(0, 1.25, 0.7)$, and place a varying number of relays along the corners and sides of a square of side length 2ℓ meters, centered at $(0, 0, 2)$. Specifically, we locate one relay at the center of the square, at $(0, 0, 2)$, and the remaining relays at either the corners: $(\ell, \ell, 2)$, $(-\ell, \ell, 2)$, $(\ell, -\ell, 2)$, and $(-\ell, -\ell, 2)$; or at the centers of the sides: $(\ell, 0, 2)$, $(0, \ell, 2)$, $(-\ell, 0, 2)$, and $(0, -\ell, 2)$, see the plan view in Fig. 9. We vary the number of relays, K, from 3 to 9 relays, and plot the achievable secrecy sum rate for each case in Fig. 10. The solid lines in the figure are when $\ell = 0.1$ meters, while the dashed lines

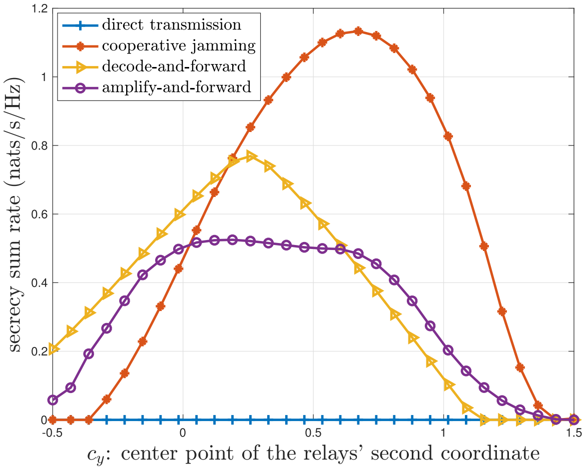


Fig. 8. Effect of the relays' distance from the eavesdropper on the secrecy sum rate. The eavesdropper is located at $(0, 1, 0.7)$, while the relays are located at $(0.1, c_y+0.1, 2)$, $(0.1, c_y-0.1, 2)$, $(0, c_y, 2)$, $(-0.1, c_y+0.1, 2)$, and $(-0.1, c_y-0.1, 2)$.

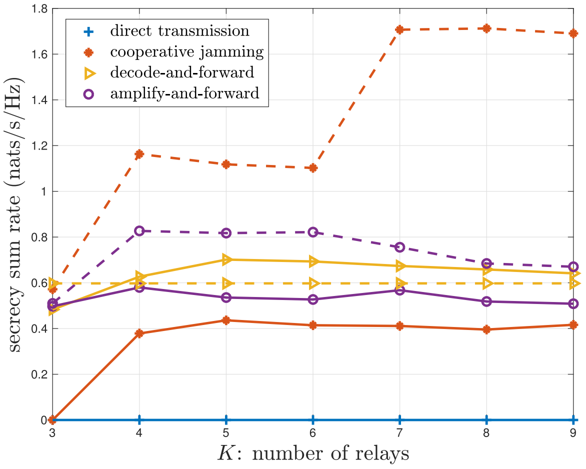


Fig. 10. Effect of number of relays on the secrecy sum rates of the proposed schemes. The eavesdropper is located at $(0, 1.25, 0.7)$. The relays are located along the corner and mid-side points of a square of side length 2ℓ meters, centered at $(0, 0, 2)$. Solid lines are when $\ell = 0.1$, and dashed lines are when $\ell = 0.5$.

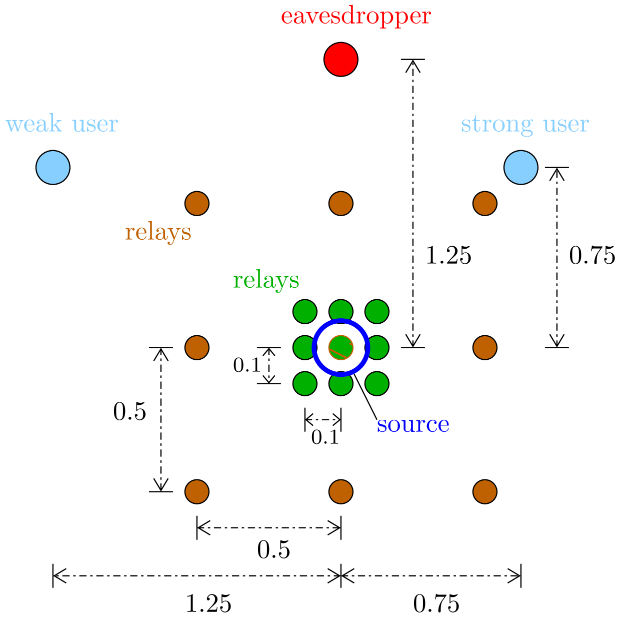


Fig. 9. Plan view of the geometric layout of the system, in which the number of relays is varying, as well as their relative distance from each other. Either the layout in green with $\ell = 0.1$, or that in brown with $\ell = 0.5$ is chosen to employ the varying number of relays.

are when $\ell = 0.5$ meters. We see from the figure that direct transmission achieves zero secrecy rates, since the eavesdropper is relatively closer to the source than the legitimate users, while all the proposed schemes achieve strictly positive secrecy sum rates. The main message conveyed by this figure, however, is that for every relaying scheme, there exists an optimal number of relays that maximizes the secrecy sum rate. Such optimal number is not necessarily the maximum number of relays available (9 in this case). The reason behind this is that when new relay LEDs are added to the system, the power share *per-relay* decreases. This might hurt the overall performance if, for instance, this newly added relay is not very well-positioned with respect to the eavesdropper, relative to the already existing ones, and ends up consuming power unnecessarily. Another observation from Fig. 10 is that the relative distance between the relays is an important system aspect that should be carefully designed to meet a desired system performance.

VIII. Conclusion and Future Directions

A VLC broadcast channel in which a transmitter communicates with two legitimate receivers in the presence of an external eavesdropper has been considered. Under an amplitude constraint, imposed to allow the LEDs to operate within their dynamic range, an achievable secrecy rate region has been derived, based on superposition coding with uniform signaling. Then, trusted cooperative half-duplex relay nodes have been introduced in order to assist with securing the data from the eavesdropper via multiple relaying schemes: cooperative jamming, decode-and-forward, and amplify-and-forward. Secure beamforming signals have been carefully designed at the relays to enhance the achievable secrecy rates. It has been shown that the best relaying scheme varies according to the distance from the transmitter (and the relays) to the eavesdropper, and also on the number of relays and their geometric layout.

Extending the approaches in this paper to the case with multiple transmitting LED fixtures and/or multiple receiving PDs would be of interest as a future direction. In addition, one could also consider deriving achievable secrecy rate regions based on different distributions other than uniform, such as discrete and truncated generalized normal distributions, that have been previously used in the literature. Another direction would be to consider the case in which the eavesdropper's location is not known at the transmitter, or known within some boundaries. In the former case, the goal would be deriving secrecy outage probabilities, while in the latter case, the goal could be deriving a worst case achievable secrecy rate region.

Appendix

A. Proof of Theorem 1

Given α, the following secrecy rates, for the strong and weak users, are achievable for this multi-receiver wiretap channel [37]:

$$c_{1,s} = \left[\mathbb{I}(x;y_1|x_2) - \mathbb{I}(x;y_e|x_2)\right]^+, \tag{60}$$

$$c_{2,s} = \left[\mathbb{I}(x_2;y_2) - \mathbb{I}(x_2;y_e)\right]^+, \tag{61}$$

where $\mathbb{I}(\cdot;\cdot)$ denotes the mutual information measure [34]. Now let the transmitted symbols x_1 and x_2 represent two independent uniformly distributed random variables on $[-A, A]$. Clearly, this satisfies the amplitude constraint in (2). Let us now drop the superscript $+$ for simplicity of presentation. We proceed by lower bounding $c_{1,s}$ as follows:

$$\begin{aligned}
c_{1,s} &\geq \mathbb{I}\left(x; h_1(\alpha x_1 + (1-\alpha)x_2) + n_1 | x_2\right) \\
&\quad - \mathbb{I}\left(x; h_e(\alpha x_1 + (1-\alpha)x_2) + n_e | x_2\right) && (62)\\
&= \mathbb{I}\left(x_1; h_1\alpha x_1 + n_1\right) - \mathbb{I}\left(x_1; h_e\alpha x_1 + n_e\right) && (63)\\
&= \mathbb{h}\left(h_1\alpha x_1 + n_1\right) - \mathbb{h}\left(h_e\alpha x_1 + n_e\right) && (64)\\
&\geq \frac{1}{2}\log\left(e^{2\mathbb{h}(h_1\alpha x_1)} + e^{2\mathbb{h}(n_1)}\right) \\
&\quad - \frac{1}{2}\log\left(2\pi e\left(h_e^2\alpha^2\frac{A^2}{3} + 1\right)\right) && (65)\\
&= \frac{1}{2}\log\left(h_1^2\alpha^2 4A^2 + 2\pi e\right) \\
&\quad - \frac{1}{2}\log\left(2\pi e\left(h_e^2\alpha^2\frac{A^2}{3} + 1\right)\right) && (66)\\
&= r_{1,s}, && (67)
\end{aligned}$$

where $\mathbb{h}(\cdot)$ in (64) denotes the differential entropy measure [34], and (65) follows by lower bounding the first (positive) term in (64) by the entropy power inequality (EPI) [34] and upper bounding the second (negative) term in (64) by plugging in a Gaussian x_1, instead of uniform, with the same variance, since Gaussian maximizes differential entropy [34]. Next, we proceed similarly to lower bound $c_{2,s}$ as follows:

$$\begin{aligned}
c_{2,s} &= \mathbb{I}\left(x_2; h_2(\alpha x_1 + (1-\alpha)x_2) + n_2\right) \\
&\quad - \mathbb{I}\left(x_2; h_e(\alpha x_1 + (1-\alpha)x_2) + n_e\right) && (68)\\
&= \mathbb{h}\left(h_2(\alpha x_1 + (1-\alpha)x_2) + n_2\right) - \mathbb{h}\left(h_2\alpha x_1 + n_2\right) \\
&\quad - \mathbb{h}\left(h_e(\alpha x_1 + (1-\alpha)x_2) + n_e\right) + \mathbb{h}\left(h_e\alpha x_1 + n_e\right) \\
& && (69)\\
&\geq \alpha\mathbb{h}\left(h_2x_1 + n_2\right) + (1-\alpha)\mathbb{h}\left(h_2x_2 + n_2\right) \\
&\quad - \mathbb{h}\left(h_2\alpha x_1 + n_2\right) - \mathbb{h}\left(h_e(\alpha x_1 + (1-\alpha)x_2) + n_e\right) \\
&\quad + \mathbb{h}\left(h_e\alpha x_1 + n_e\right) && (70)\\
&\geq \frac{1}{2}\log\left(e^{2\mathbb{h}(h_2x_1)} + e^{2\mathbb{h}(n_2)}\right) \\
&\quad - \frac{1}{2}\log\left(2\pi e\left(h_2^2\alpha^2\frac{A^2}{3} + 1\right)\right) \\
&\quad - \frac{1}{2}\log\left(2\pi e\left(h_e^2\alpha^2\frac{A^2}{3} + h_e^2(1-\alpha)^2\frac{A^2}{3} + 1\right)\right) \\
&\quad + \frac{1}{2}\log\left(e^{2\mathbb{h}(h_e\alpha x_1)} + e^{2\mathbb{h}(n_e)}\right) && (71)\\
&\geq \frac{1}{2}\log\left(e^{2\mathbb{h}(h_2x_1)} + e^{2\mathbb{h}(n_2)}\right) \\
&\quad - \frac{1}{2}\log\left(2\pi e\left(h_2^2\alpha^2\frac{A^2}{3} + 1\right)\right) \\
&\quad - \frac{1}{2}\log\left(2\pi e\left(h_e^2\frac{A^2}{3} + 1\right)\right) \\
&\quad + \frac{1}{2}\log\left(e^{2\mathbb{h}(h_e\alpha x_1)} + e^{2\mathbb{h}(n_e)}\right) && (72)\\
&= \frac{1}{2}\log\left(h_2^2 4A^2 + 2\pi e\right) \\
&\quad - \frac{1}{2}\log\left(2\pi e\left(h_2^2\alpha^2\frac{A^2}{3} + 1\right)\right) \\
&\quad - \frac{1}{2}\log\left(2\pi e\left(h_e^2\frac{A^2}{3} + 1\right)\right) \\
&\quad + \frac{1}{2}\log\left(h_2^2\alpha^2 4A^2 + 2\pi e\right) && (73)\\
&= r_{2,s}, && (74)
\end{aligned}$$

where (70) follows by Jensen's inequality (concavity of differential entropy) [34]; (71) follows by using EPI to lower bound the positive terms of (70) together with the fact that $h_2x_1 + n_2$ and $h_2x_2 + n_2$ have the same distribution, and plugging in a Gaussian x_1 and x_2, instead of uniform, with the same variances to upper bound the negative terms of (70); and (72) follows since $\alpha \leq 1$. This concludes the proof.

B. Proof of Theorem 2

We first note that, different from direct transmission, over here we have another random variable z involved in the calculations. To emphasize the difference, we denote the secrecy rates in (60) and (61) by $c_{1,s}^J$ and $c_{2,s}^J$, respectively. We now proceed with the same approach as that followed in the proof of Theorem 1. Specifically, we let x_1 and x_2 be two independent uniformly distributed random variables on $[-A_\gamma, A_\gamma]$, and let z be uniformly distributed on $\left[-\bar{A}, \bar{A}\right]$, independently of x_1 and x_2. We then expand the mutual information terms constituting $c_{1,s}^J$ and $c_{2,s}^J$ in terms of differential entropy, lower bound positive terms by EPI (and Jensen's inequality if need be), and upper bound negative terms by plugging in Gaussian random variables with the same variances, instead of uniform. Specific justifications of intermediate steps are as in the proof of Theorem 1 and are thus omitted for brevity. We also drop the superscript $+$ for convenience.

A lower bound on $c_{1,s}^J$ is now given by

$$\begin{aligned}
c_{1,s}^J &= \mathbb{I}(x_1; h_1\alpha x_1 + n_1) - \mathbb{I}\left(x_1; h_e\alpha x_1 + \mathbf{g}_e^T\mathbf{J}_o z + n_e\right) \\
& && (75)\\
&= \mathbb{h}(h_1\alpha x_1 + n_1) - \mathbb{h}(n_1) - \mathbb{h}\left(h_e\alpha x_1 + \mathbf{g}_e^T\mathbf{J}_o z + n_e\right) \\
&\quad + \mathbb{h}\left(\mathbf{g}_e^T\mathbf{J}_o z + n_e\right) && (76)\\
&\geq \frac{1}{2}\log\left(e^{2\mathbb{h}(h_1\alpha x_1)} + e^{2\mathbb{h}(n_1)}\right) - \frac{1}{2}\log(2\pi e) \\
&\quad - \frac{1}{2}\log\left(2\pi e\left(h_e^2\alpha^2\frac{A_\gamma^2}{3} + \left(\mathbf{g}_e^T\mathbf{J}_o\right)^2\frac{\bar{A}^2}{3} + 1\right)\right) \\
&\quad + \frac{1}{2}\log\left(e^{2\mathbb{h}\left(\mathbf{g}_e^T\mathbf{J}_o z\right)} + e^{2\mathbb{h}(n_e)}\right) && (77)\\
&= \frac{1}{2}\log\left(h_1^2\alpha^2 4A_\gamma^2 + 2\pi e\right) - \frac{1}{2}\log(2\pi e)
\end{aligned}$$

$$
\begin{aligned}
&-\frac{1}{2}\log\left(2\pi e\left(h_e^2\alpha^2\frac{A_\gamma^2}{3}+\left(\mathbf{g}_e^T\mathbf{J}_o\right)^2\frac{\bar{A}^2}{3}+1\right)\right)\\
&+\frac{1}{2}\log\left(\left(\mathbf{g}_e^T\mathbf{J}_o\right)^2\alpha^2 4\bar{A}^2+2\pi e\right) \qquad (78)\\
&= r_{1,s}^J. \qquad (79)
\end{aligned}
$$

Similarly, we lower bound $c_{2,s}^J$ as follows:

$$
\begin{aligned}
c_{2,s}^J &= \mathbb{I}\left(x_2; h_2(\alpha x_1+(1-\alpha)x_2)+n_2\right)\\
&\quad -\mathbb{I}\left(x_2; h_e(\alpha x_1+(1-\alpha)x_2)+\mathbf{g}_e^T\mathbf{J}_o z+n_e\right) \qquad (80)\\
&= \mathbb{h}\left(h_2(\alpha x_1+(1-\alpha)x_2)+n_2\right)-\mathbb{h}\left(h_2\alpha x_1+n_2\right)\\
&\quad -\mathbb{h}\left(h_e(\alpha x_1+(1-\alpha)x_2)+\mathbf{g}_e^T\mathbf{J}_o z+n_e\right)\\
&\quad +\mathbb{h}\left(h_e\alpha x_1+\mathbf{g}_e^T\mathbf{J}_o z+n_e\right) \qquad (81)\\
&\geq \alpha\mathbb{h}\left(h_2x_1+n_2\right)+(1-\alpha)\mathbb{h}\left(h_2x_2+n_2\right)\\
&\quad -\mathbb{h}\left(h_2\alpha x_1+n_2\right)\\
&\quad -\mathbb{h}\left(h_e(\alpha x_1+(1-\alpha)x_2)+\mathbf{g}_e^T\mathbf{J}_o z+n_e\right)\\
&\quad +\mathbb{h}\left(h_e\alpha x_1+\mathbf{g}_e^T\mathbf{J}_o z+n_e\right) \qquad (82)\\
&\geq \frac{1}{2}\log\left(e^{2\mathbb{h}(h_2x_1)}+e^{2\mathbb{h}(n_2)}\right)\\
&\quad -\frac{1}{2}\log\left(2\pi e\left(h_2^2\alpha^2\frac{A_\gamma^2}{3}+1\right)\right)\\
&\quad -\frac{1}{2}\log\left(2\pi e\left(h_e^2\alpha^2\frac{A_\gamma^2}{3}+h_e^2(1-\alpha)^2\frac{A_\gamma^2}{3}\right.\right.\\
&\qquad\qquad \left.\left.+\left(\mathbf{g}_e^T\mathbf{J}_o\right)^2\frac{\bar{A}^2}{3}+1\right)\right)\\
&\quad +\frac{1}{2}\log\left(e^{2\mathbb{h}(h_e\alpha x_1)}+e^{2\mathbb{h}\left(\mathbf{g}_e^T\mathbf{J}_o z\right)}+e^{2\mathbb{h}(n_e)}\right) \qquad (83)\\
&\geq \frac{1}{2}\log\left(e^{2\mathbb{h}(h_2x_1)}+e^{2\mathbb{h}(n_2)}\right)\\
&\quad -\frac{1}{2}\log\left(2\pi e\left(h_2^2\alpha^2\frac{A_\gamma^2}{3}+1\right)\right)\\
&\quad -\frac{1}{2}\log\left(2\pi e\left(h_e^2\frac{A_\gamma^2}{3}+\left(\mathbf{g}_e^T\mathbf{J}_o\right)^2\frac{\bar{A}^2}{3}+1\right)\right)\\
&\quad +\frac{1}{2}\log\left(e^{2\mathbb{h}(h_e\alpha x_1)}+e^{2\mathbb{h}\left(\mathbf{g}_e^T\mathbf{J}_o z\right)}+e^{2\mathbb{h}(n_e)}\right) \qquad (84)\\
&= \frac{1}{2}\log\left(h_2^2 4A_\gamma^2+2\pi e\right)\\
&\quad -\frac{1}{2}\log\left(2\pi e\left(h_2^2\alpha^2\frac{A_\gamma^2}{3}+1\right)\right)\\
&\quad -\frac{1}{2}\log\left(2\pi e\left(h_e^2\frac{A_\gamma^2}{3}+\left(\mathbf{g}_e^T\mathbf{J}_o\right)^2\frac{\bar{A}^2}{3}+1\right)\right)\\
&\quad +\frac{1}{2}\log\left(h_2^2\alpha^2 4A_\gamma^2+\left(\mathbf{g}_e^T\mathbf{J}_o\right)^2\alpha^2 4\bar{A}^2+2\pi e\right) \qquad (85)\\
&= r_{2,s}^J. \qquad (86)
\end{aligned}
$$

This concludes the proof.

C. Proof of Theorem 3

We let the relays employ the same decoding technique of the strong user: first decode the weak user's message by treating the strong user's interfering signal as noise, and then use successive interference cancellation to decode the strong user's message. Using the decode-and-froward lower bound in [38, Th. 16.2], the following secrecy rates are achievable:

$$
\begin{aligned}
c_{1,s}^{DF} &= \frac{1}{2}\Big[\min\Big\{\mathbb{I}\left(x,x_r;y_1,y_1^r|x_2,\tilde{x}_2\right),\min_i\mathbb{I}\left(x_1;y_{r,i}|x_2\right)\Big\}\\
&\qquad -\mathbb{I}(x;y_e|x_2)\Big]^+, \qquad (87)\\
c_{2,s}^{DF} &= \frac{1}{2}\Big[\min\Big\{\mathbb{I}\left(x_2,\tilde{x}_2;y_2,y_2^r\right),\min_i\mathbb{I}\left(x_2;y_{r,i}\right)\Big\}\\
&\qquad -\mathbb{I}(x_2;y_e)\Big]^+, \qquad (88)
\end{aligned}
$$

where the extra $\frac{1}{2}$ term is due to sending the same information over two phases of equal durations. By the independence of x_j and $\tilde{x}_j$, $j=1,2$, we have

$$
\begin{aligned}
\mathbb{I}(x_1,\tilde{x}_1;y_1,y_1^r|x_2,\tilde{x}_2) &= \mathbb{I}(x_1;h_1\alpha x_1+n_1)\\
&\quad +\mathbb{I}\left(\tilde{x}_1;\mathbf{g}_1^T\mathbf{d}_o\alpha\tilde{x}_1+n_1^r\right), \qquad (89)\\
\mathbb{I}(x_2,\tilde{x}_2;y_2,y_2^r) &= \mathbb{I}(x_2;h_2\alpha(\alpha x_1+(1-\alpha)x_2)+n_2)\\
&\quad +\mathbb{I}\left(\tilde{x}_2;\mathbf{g}_2^T\mathbf{d}_o(\alpha\tilde{x}_1+(1-\alpha)\tilde{x}_2)+n_2^r\right). \qquad (90)
\end{aligned}
$$

To derive the lower bounds on $c_{1,s}^{DF}$ and $c_{2,s}^{DF}$, we proceed as in the proof of Theorem 1 by lower bounding the positive terms above by EPI (and Jensen's inequality if need be), and upper bounding the negative terms above by plugging in Gaussian random variables with the same variances instead of uniform. This directly gives $r_{1,s}^{DF}$ and $r_{2,s}^{DF}$. Specific details are merely the same as in the proof of Theorem 1 and are omitted for brevity.

D. Proof of Theorem 4

We note that the jth user, $j=1,2$, can view the system as the following 1×2 SIMO system:

$$
\begin{bmatrix} y_j \\ y_j^r \end{bmatrix} = \begin{bmatrix} h_j \\ \mathbf{g}_j^T\mathtt{diag}\left(\mathbf{h}_r\right)\mathbf{a}_o \end{bmatrix} x + \begin{bmatrix} n_j \\ \tilde{n}_j^r \end{bmatrix}, \qquad (91)
$$

where the noise term $\tilde{n}_j^r \triangleq \mathbf{g}_j^T\mathtt{diag}\left(\mathbf{n}_r\right)\mathbf{a}_o+n_j^r$, which is $\sim\mathcal{N}\left(0,1+\left(\mathbf{g}_j^T\mathbf{a}_o\right)^2\right)$. The jth user then applies the capacity achieving maximal ratio combining [39] to get the following sufficient statistic:

$$
\begin{aligned}
\tilde{y}_j &\triangleq h_jy_j+\frac{\mathbf{g}_j^T\mathtt{diag}\left(\mathbf{h}_r\right)\mathbf{a}_o}{1+\left(\mathbf{g}_j^T\mathbf{a}_o\right)^2}y_j^r \qquad (92)\\
&\triangleq h_jy_j+\frac{h_{j,r}}{\sigma_{j,r}^2}y_j^r. \qquad (93)
\end{aligned}
$$

Therefore, the following secrecy rates are now achievable:

$$
\begin{aligned}
c_{1,s}^{AF} &= \frac{1}{2}\left[\mathbb{I}\left(x;\tilde{y}_1|x_2\right)-\mathbb{I}(x;y_e|x_2)\right]^+, \qquad (94)\\
c_{2,s}^{AF} &= \frac{1}{2}\left[\mathbb{I}\left(x_2;\tilde{y}_2\right)-\mathbb{I}(x_2;y_e)\right]^+, \qquad (95)
\end{aligned}
$$

where the extra $\frac{1}{2}$ term is due to sending the same information over two phases of equal durations, as in the decode-and-forward scheme. We now proceed with lower bounding the positive mutual information terms in (94) and (95); the negative terms are handled exactly as in the proof of Theorem 1. For the strong user, we have

$$\begin{aligned}
&\mathbb{I}\left(x;\tilde{y}_1|x_2\right)\\
&= \mathbb{h}\left(\left(h_1^2+\frac{h_{1,r}^2}{\sigma_{1,r}^2}\right)\alpha x_1 + h_1 n_1 + \frac{h_{1,r}}{\sigma_{1,r}^2}\tilde{n}_1^r\right)\\
&\quad -\mathbb{h}\left(h_1 n_1 + \frac{h_{1,r}}{\sigma_{1,r}^2}\tilde{n}_1^r\right) &(96)\\
&\geq \frac{1}{2}\log\left(e^{2\mathbb{h}\left(\left(h_1^2+\frac{h_{1,r}^2}{\sigma_{1,r}^2}\right)\alpha x_1\right)} + e^{2\mathbb{h}(h_1 n_1)} + e^{2\mathbb{h}\left(\frac{h_{1,r}}{\sigma_{1,r}^2}\tilde{n}_1^r\right)}\right)\\
&\quad -\frac{1}{2}\log\left((2\pi e)\left(h_1^2+\frac{h_{1,r}^2}{\sigma_{1,r}^2}\right)\right) &(97)\\
&= \frac{1}{2}\log\left(\left(h_1^2+\frac{h_{1,r}^2}{\sigma_{1,r}^2}\right)^2\alpha^2 4A_\gamma^2 + (2\pi e)\left(h_1^2+\frac{h_{1,r}^2}{\sigma_{1,r}^2}\right)\right)\\
&\quad -\frac{1}{2}\log\left((2\pi e)\left(h_1^2+\frac{h_{1,r}^2}{\sigma_{1,r}^2}\right)\right) &(98)\\
&= \frac{1}{2}\log\left(1+\frac{2\kappa_1^2\alpha^2 A_\gamma^2}{\pi e}\right). &(99)
\end{aligned}$$

Similarly, for the weak user, we have

$$\begin{aligned}
&\mathbb{I}\left(x_2;\tilde{y}_2\right)\\
&= \mathbb{h}\left(\left(h_2^2+\frac{h_{2,r}^2}{\sigma_{2,r}^2}\right)(\alpha x_1 + (1-\alpha)x_2) + h_2 n_2 + \frac{h_{2,r}}{\sigma_{2,r}^2}\tilde{n}_2^r\right)\\
&\quad -\mathbb{h}\left(\left(h_2^2+\frac{h_{2,r}^2}{\sigma_{2,r}^2}\right)\alpha x_1 + h_2 n_2 + \frac{h_{2,r}}{\sigma_{2,r}^2}\tilde{n}_2^r\right) &(100)\\
&\geq \alpha\mathbb{h}\left(\left(h_2^2+\frac{h_{2,r}^2}{\sigma_{2,r}^2}\right)x_1 + h_2 n_2 + \frac{h_{2,r}}{\sigma_{2,r}^2}\tilde{n}_2^r\right)\\
&\quad +(1-\alpha)\mathbb{h}\left(\left(h_2^2+\frac{h_{2,r}^2}{\sigma_{2,r}^2}\right)x_2 + h_2 n_2 + \frac{h_{2,r}}{\sigma_{2,r}^2}\tilde{n}_2^r\right)\\
&\quad -\frac{1}{2}\log\left((2\pi e)\left(\left(h_2^2+\frac{h_{2,r}^2}{\sigma_{2,r}^2}\right)^2\frac{A_\gamma^2}{3} + h_2^2 + \frac{h_{2,r}^2}{\sigma_{2,r}^2}\right)\right) &(101)\\
&\geq \frac{1}{2}\log\left(e^{2\mathbb{h}\left(\left(h_2^2+\frac{h_{2,r}^2}{\sigma_{2,r}^2}\right)x_1\right)} + e^{2\mathbb{h}(h_2 n_2)} + e^{2\mathbb{h}\left(\frac{h_{2,r}}{\sigma_{2,r}^2}\tilde{n}_2^r\right)}\right)\\
&\quad -\frac{1}{2}\log\left((2\pi e)\left(\left(h_2^2+\frac{h_{2,r}^2}{\sigma_{2,r}^2}\right)^2\frac{A_\gamma^2}{3} + h_2^2 + \frac{h_{2,r}^2}{\sigma_{2,r}^2}\right)\right) &(102)\\
&= \frac{1}{2}\log\left(\left(h_2^2+\frac{h_{2,r}^2}{\sigma_{2,r}^2}\right)^2 4A_\gamma^2 + (2\pi e)\left(h_2^2+\frac{h_{2,r}^2}{\sigma_{2,r}^2}\right)\right)\\
&\quad -\frac{1}{2}\log\left((2\pi e)\left(\left(h_2^2+\frac{h_{2,r}^2}{\sigma_{2,r}^2}\right)^2\frac{A_\gamma^2}{3} + h_2^2 + \frac{h_{2,r}^2}{\sigma_{2,r}^2}\right)\right) &(103)\\
&= \frac{1}{2}\log\left(\frac{1+\frac{2\kappa_2^2 A_\gamma^2}{\pi e}}{1+\frac{\kappa_2^2\alpha^2 A_\gamma^2}{3}}\right). &(104)
\end{aligned}$$

This concludes the proof.

References

[1] A. Arafa, E. Panayirci, and H. V. Poor, "Relay-aided secure broadcasting for VLC," in *Proc. IEEE GlobalSIP*, Nov. 2018, pp. 1286–1290.

[2] 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, Feb. 2004.

[3] J. Grubor, O. C. G. Jamett, K.-D. Langer, J. W. Walewski, and S. Randel, "High-speed wireless indoor communication via visible light," *ITG Facherícht*, vol. 198, pp. 203–208, Mar. 2007.

[4] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," *Proc. Nat. Acad. Sci. USA*, vol. 114, no. 1, pp. 19–26, Jan. 2017.

[5] A. Mostafa and L. Lampe, "Securing visible light communications via friendly jamming," in *Proc. IEEE Globecom*, Dec. 2014, pp. 524–529.

[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*, Dec. 2015, pp. 1165–1169.

[7] A. Mostafa and L. Lampe, "Physical-layer security for MISO visible light communication channels," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 9, pp. 1806–1818, Sep. 2015.

[8] A. Mostafa and L. Lampe, "Optimal and robust beamforming for secure transmission in MISO visible-light communication links," *IEEE Trans. Signal Process.*, vol. 64, no. 24, pp. 6501–6516, Dec. 2016.

[9] 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*, Dec. 2016, pp. 1–7.

[10] 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*, Dec. 2016, pp. 970–974.

[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*, Mar. 2017, pp. 1–6.

[12] 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.*, vol. 22, no. 7, pp. 1382–1385, Jul. 2018.

[13] M. A. Arfaoui, A. Ghrayeb, and C. Assi, "On the achievable secrecy rate of the MIMO VLC Gaussian wiretap channel," in *Proc. IEEE PIMRC*, Oct. 2017, pp. 1–5.

[14] G. Pan, J. Ye, and Z. Ding, "On secure VLC systems with spatially random terminals," *IEEE Commun. Lett.*, vol. 21, no. 3, pp. 492–495, Mar. 2017.

[15] 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, pp. 475–480.

[16] 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.*, vol. 7, no. 6, pp. 768–771, Oct. 2018.

[17] 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*, Jun. 2017, pp. 258–263.

[18] G. Pan, J. Ye, and Z. Ding, "Secure hybrid VLC-RF systems with light energy harvesting," *IEEE Trans. Commun.*, vol. 65, no. 10, pp. 4348–4359, Oct. 2017.

[19] 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.

[20] 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.

[21] S. Cho, G. Chen, H. Chun, J. P. Coon, and D. O'Brien, "Impact of multipath reflections on secrecy in VLC systems with randomly located eavesdroppers," in *Proc. IEEE WCNC*, Apr. 2018, pp. 1–6.

[22] T. V. Pham and A. T. Pham, "On the secrecy sum-rate of MU-VLC broadcast systems with confidential messages," in *Proc. IEEE CSNDSP*, Jul. 2016, pp. 1–6.

[23] 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*, Dec. 2017, pp. 1–6.

[24] M. Safari and M. Uysal, "Relay-assisted free-space optical communication," *IEEE Trans. Wireless Commun.*, vol. 7, no. 12, pp. 5441–5449, Dec. 2008.

[25] F. E. Alsaadi, M. Nikkar, and J. M. H. Elmirghani, "Adaptive mobile optical wireless systems employing a beam clustering method, diversity detection, and relay nodes," *IEEE Trans. Commun.*, vol. 58, no. 3, pp. 869–879, Mar. 2010.

[26] H. Yang and A. Pandharipande, "Full-duplex relay VLC in LED lighting linear system topology," in *Proc. IEEE IECON*, Nov. 2013, pp. 6075–6080.

[27] H. Yang and A. Pandharipande, "Full-duplex relay VLC in LED lighting triangular system topology," in *Proc. ISCCSP*, May 2014, pp. 85–88.

[28] A. T. Hussein and J. M. H. Elmirghani, "10 Gbps mobile visible light communication system employing angle diversity, imaging receivers, and relay nodes," *J. Opt. Commun. Netw.*, vol. 7, no. 8, pp. 718–735, Aug. 2015.

[29] R. C. Kizilirmak, O. Narmanlioglu, and M. Uysal, "Relay-assisted OFDM-based visible light communications," *IEEE Trans. Commun.*, vol. 63, no. 10, pp. 3765–3778, Oct. 2015.

[30] O. Narmanlioglu, R. C. Kizilirmak, F. Miramirkhani, and M. Uysal, "Cooperative visible light communications with full-duplex relaying," *IEEE Photon. J.*, vol. 9, no. 3, pp. 1–11, Jun. 2017.

[31] C. Zhang, J. Ye, G. Pan, and Z. Ding, "Cooperative hybrid VLC-RF systems with spatially random terminals," *IEEE Trans. Commun.*, vol. 66, no. 12, pp. 6396–6408.

[32] Z. Ding *et al.*, "Application of non-orthogonal multiple access in LTE and 5G networks," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 185–191, Feb. 2017.

[33] M. Vaezi, Z. Ding, and H. V. Poor, Eds., *Multiple Access Techniques for 5G Wireless Networks and Beyond*. New York, NY, USA: Springer, 2018.

[34] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Hoboken, NJ, USA: Wiley, 2006.

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

[36] W. Dinkelbach, "On nonlinear fractional programming," *Manage. Sci.*, vol. 13, no. 7, pp. 492–498, Mar. 1967.

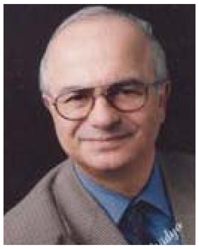
[37] E. Ekrem and S. Ulukus, "The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2083–2114, Apr. 2011.

[38] A. El Gamal and Y.-H. Kim, *Network Information Theory*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[39] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

Ahmed Arafa (S'13–M'17) received the B.Sc. degree (distinction with honor) in electrical engineering from Alexandria University, Egypt, in 2010, the M.Sc. degree in wireless technologies from the Wireless Intelligent Networks Center, Nile University, Egypt, in 2012, and the Ph.D. degree in electrical engineering from the University of Maryland at College Park, in 2017. He is currently a Post-Doctoral Research Associate with the Electrical Engineering Department, Princeton University.

His research interests are in communication theory, information theory and networks, with recent focus on energy harvesting communications, age of information, physical layer security, non-orthogonal multiple access systems, and visible light communications. He was a recipient of the Distinguished Dissertation Fellowship from the Department of Electrical and Computer Engineering, University of Maryland, in 2017, for his Ph.D. thesis work on optimal energy management policies in energy harvesting communication networks with system costs.



Erdal Panayirci (M'80–SM'91–F'03–LF'06) received the Diploma Engineering degree in electrical engineering from Istanbul Technical University, Istanbul, Turkey, and the Ph.D. degree in electrical engineering and system science from Michigan State University, MI, USA. He is currently a Professor of electrical engineering and the Head of the Electrical and Electronics Engineering Department, Kadir Has University, Istanbul. His recent research interests include communication theory, synchronization, advanced signal processing techniques and their applications to wireless electrical, underwater, and optical communications. From 2008 to 2009 and from 2017 to 2018, he was with the Department of Electrical Engineering, Princeton University, NJ, USA, working on new channel estimation and equalization algorithms for communication systems and on visible light communications. He has published extensively in leading scientific journals and international conferences and co-authored the book *Principles of Integrated Maritime Surveillance Systems* (Boston, MA, USA: Kluwer Academic, 2000).

Dr. Panayirci has served and is currently serving as a member of IEEE Fellow Committee. He is a member of the IEEE GLOBECOM/ICC Management and Strategy Standing Committee. He was the Technical Program Co-Chair of the IEEE International Conference on Communications (ICC) and the Technical Program Chair of the IEEE PIMRC, Istanbul, in 2006 and 2010, respectively. He was the Executive Vice Chairman of the IEEE Wireless Communications and Networking Conference, Istanbul, in 2014. He is the General Co-Chair of the IEEE PIMRC, Istanbul, in 2019. He has been the Principal Coordinator of a 6th and 7th Frame European Project called Network of Excellent on Wireless Communications and WIMAGIC Strep project for two years, representing Kadir Has University. He was an Editor of the IEEE TRANSACTIONS ON COMMUNICATIONS in synchronizations and equalizations from 1995 to 2000.

H. Vincent Poor (S'72–M'77–SM'82–F'87) received the Ph.D. degree in EECS from Princeton University in 1977. From 1977 to 1990, he was on the faculty of the University of Illinois at Urbana–Champaign. Since 1990, he has been on the faculty at Princeton, where he is currently the Michael Henry Strater University Professor of Electrical Engineering. From 2006 to 2016, he served as the Dean of Princeton's School of Engineering and Applied Science. He has also held visiting appointments at several other universities, including most recently at Berkeley and Cambridge. His research interests are in the areas of information theory and signal processing, and their applications in wireless networks, energy systems and related fields. Among his publications in these areas is the recent book *Information Theoretic Security and Privacy of Information Systems* (Cambridge University Press, 2017).

Dr. Poor is a Member of the National Academy of Engineering and the National Academy of Sciences, and is a Foreign Member of the Chinese Academy of Sciences, the Royal Society, and other national and international academies. He received the Marconi and Armstrong Awards of the IEEE Communications Society in 2007 and 2009, respectively. Recent recognition of his work includes the 2017 IEEE Alexander Graham Bell Medal, Honorary Professorships at Peking University and Tsinghua University, both conferred in 2017, and a D.Sc. *honoris causa* from Syracuse University in 2017.