Enhancement of Physical Layer Security with Simultaneous Beamforming and Jamming for Visible Light Communication Systems

Sunghwan Cho, *Student Member, IEEE,* Gaojie Chen, *Senior Member, IEEE,* and Justin P. Coon, *Senior Member, IEEE*

***Abstract*—This paper considers physical layer security enhancement mechanisms that utilize simultaneous beamforming and jamming in visible light communication (VLC) systems with a *randomly* located eavesdropper under the assumption that there are multiple light-emitting diode (LED) transmitters and one intended user. When an eavesdropper with an augmented front-end receiver is present, the jamming is very useful for preventing the eavesdropper from wiretapping the information since it is not possible to extract only the information component from the received signal if the jamming signal is random. Thus, in this paper, an optimization problem is formulated with a focus on the signal-to-interference-plus-noise ratio for the legitimate link, and it is solved by a heuristic method called the concave-convex procedure. Then, a ternary scheme is proposed, which is less complicated than the full (joint) scheme, and it is optimized by adopting a formulation based on an assignment problem, the solution of which is effectively obtained by the so-called *tabu search* procedure. Additionally, the problem of maximizing the average secrecy rate is investigated by utilizing a continuous LED model, which significantly relaxes the complication that rises from calculating the expectation with respect to the location of the eavesdropper. Our analysis and simulation results show that the proposed simultaneous beamforming and jamming strategies (both joint and ternary) are good proxies for maximizing the average secrecy rate by utilizing the statistical information on the eavesdropper's random location.**

***Index Terms*—Physical layer security, visible light communication, beamforming, jamming, average secrecy rate.**

I. Introduction

Over the past decade, as the number of mobile devices connected to the Internet has increased, with primary user activities including data-intensive HD video streaming and cloud-based service access, the capacity demand on the radio access network has been steadily increasing. To satisfy this demand, wireless providers are deploying additional access infrastructures that rely on new cells and WiFi endpoints. However, it has proved challenging to improve data rate and reduce latency given the limited range of available radio frequency (RF) spectrum. Moreover, a large number of access points deployed in congested public areas cause high interference among themselves, which results in a degradation in the performance of the communication network [1]–[3].

Spurred by these issues, many researchers and engineers have further explored new air interfaces and spectrum, such as light and extremely high-frequency waves. Visible light communication (VLC) systems, which utilize visible light as the communication medium and exploit the light infrastructure currently being used for illumination, have gained popularity in academia and industry. VLC has a few advantages in terms of unlicensed wide bandwidth, high area spectral efficiency, and high security [3], where the last two advantages come from the fact that visible light cannot penetrate opaque walls, and the area being illuminated by a certain light-emitting diode (LED) can be controlled and regulated by adjusting the LED emission pattern.

At the same time, in VLC systems, network security remains an important challenge that needs to be studied further. In large and crowded rooms, such as offices, libraries, and shopping malls, there is always the possibility that an eavesdropper can wiretap the information signal in the air. Physical layer security (PLS) is a set of techniques that allows a transmitter and a legitimate receiver to transmit and receive important data securely by utilizing channel randomness. In PLS, if the capacity of the intended data transmission channel is higher than that of the eavesdropping channel, the data can be securely and reliably transmitted at a rate close to the difference in their capacities, i.e., the so-called *secrecy capacity*, so that only the intended receiver can successfully decode the data [4]. Since Wyner's seminal work [5], numerous PLS enhancement techniques for RF systems have been studied, including beamforming, antenna selection, artificial interference, etc. [6]–[8].

In the meanwhile, to improve the PLS of VLC systems, many PLS techniques for VLC systems have been studied. Specifically, an extensive study has been first performed by Mostafa et al. [9]–[13]. In [9], they analyzed the achievable secrecy rates for the cases of both single-input, single-output (SISO) and multiple-input, single-output (MISO) and proposed an LED beamforming. Also, they developed null-steering, artificial noise, and friendly jamming strategies when an eavesdropper's channel state information (CSI) is initially present and then absent at the transmitter [10], [11]. Moreover, in [12], they utilized the excessive spatial degrees of freedom offered by a large number of LEDs to direct the main lobe, allowing the LEDs to transmit an important data only to the intended user being located in an insecurity zone. In [13], the beamforming weight vector maximizing the achievable secrecy rate was designed and solved by converting a non-convex opti-

S. Cho and J. P. Coon are with the Department of Engineering Science, University of Oxford, Oxford, OX1 3PJ, U.K. (e-mail: {sunghwan.cho, justin.coon}@eng.ox.ac.uk).

G. Chen is with the Department of Engineering, University of Leicester, Leicester, LE1 7RH, U.K. (e-mail: gaojie.chen@leicester.ac.uk).

This work was supported by EPSRC grant number EP/N002350/1.

mization problem into a solvable quasi-convex search problem. In addition, Alouini et al. investigated the secrecy rates with various input distributions under the amplitude constraint on the input signal [14], [15]. Particularly, in [14], the secrecy rate with the cooperative jamming scheme was analyzed when the truncated Gaussian input distribution was utilized. In [15], the authors investigated the secrecy rate for various input signaling distributions, including the truncated generalized normal and uniform distributions, via transmit beamforming and artificial noise schemes. Also, Pham et al. studied the PLS for multiuser MISO VLC systems utilizing zero-forcing and artificial noise-aided precoding, respectively [16], [17]. In [18], Arfaoui et al. proposed various precoding schemes for maximizing the max-min fairness, the harmonic mean, the proportional fairness, and the weighted fairness, respectively. Particularly, an achievable secrecy rate was provided for the system as a function of the precoding matrix. Also, in [19] and [20], the secrecy outage probability (SOP) was analyzed utilizing stochastic geometry when eavesdroppers are randomly distributed and a beamforming scheme that does not require the locations or CSI of eavesdroppers was proposed, respectively. Also, in [21], the secrecy performance in VLC in the presence of randomly located colluding eavesdroppers was investigated. Please refer to [22], [23] for further details on PLS for VLC systems.

On the one hand, a practical and feasible VLC eavesdropping scenario is that the eavesdropper augments its receive capability by, for example, increasing an area of a photodiode (PD), adopting a high gain optical lens, and accurately adjusting the receiver's orientation toward the LED transmitter. For example, in [24], a telescope was used to increase the gain of the receiver in an experimental test, which showed that VLC channels can be eavesdropped with a high-quality receiver even at a far distance. In the presence of an eavesdropper equipped with a better receiver than the intended user, a secrecy outage can occur with a high probability. To cope with this scenario, multiple jamming or artificial noise schemes for VLC systems were proposed in [10], [11], [14], [15], [25]. This is a powerful and practical approach to securing VLC systems since even eavesdroppers with powerful receiver architectures cannot distinguish between the random information jamming signals.

To date, almost all works on jamming in VLC systems have assumed that the locations and/or the CSI of eavesdroppers are available at the transmitter, which may not be practical. This paper deviates from this assumption by proposing a joint strategy of beamforming and jamming, which can be implemented in the presence of a *randomly* located eavesdropper, i.e., it does not require knowledge of the exact location or the CSI of an eavesdropper, instead only requiring the statistical information of the location of the eavesdropper.

On the other hand, [10], [11] also proposed user-friendly jamming strategies assuming that LED transmitters do not retain knowledge of the precise location of an eavesdropper. However, they have the limitations on their performance and assumption. More specifically, in the artificial noise scheme [10], the LEDs transmit randomly-generated noise symbols in the nullspace of the intended user with the hope that interference is caused at the eavesdropper site. However, this scheme left the resulting secrecy performance to luck depending on the nullspace of the intended user, thus it does not always perform in a way that maximizes the secrecy performance[1]. When engineering secure VLC systems, the inconstant secrecy performance changing with the nullspace of the intended user may cause difficulties in determining properties of a wiretap code [4]. Also, the friendly jamming scheme in [11] assumed that an eavesdropper is expected or permitted to exist within a certain *bounded* area known to the jammers. Then, they formulated the max-min optimization problem maximizing the worst-case secrecy rate over all the channel realizations of the bounded eavesdropper. However, in large open spaces, it would be impractical to anticipate or restrict the region of an eavesdropper's possible location, since the eavesdropper can be located anywhere, even at a far distance, being equipped with a high-quality receiver trying to escape the vigilance of the legitimate user. In contrast, our proposed scheme is the approach that *maximizes* the secrecy performance (not leaving to luck) by simultaneously utilizing the beamforming and jamming and does not set any constraint on the possible location of the eavesdropper, while requires only the statistical information on the eavesdropper's location. In practice, the statistical information on the location of an eavesdropper can be effectively acquired by analyzing the user behavior characteristics and the layout of the room. Moreover, note that the uniform distribution on the eavesdropper's location, as we will assume in later sections, means that the eavesdropper's location is completely random (unknown), which is the worst case from the secrecy viewpoint [26], [27].

Firstly, we formulate the optimization problem for the beamforming and jamming vectors that maximize the signal-to-interference-plus-noise ratio (SINR) of a legitimate user while suppressing the SINR of an eavesdropper. Since the optimization problem is not convex, we utilize a heuristic method called the concave-convex procedure (CCP) [28] to find the local solution. However, due to its high computational complexity when a large number of transmitters is considered, we propose a simpler version of the joint scheme called the *ternary scheme*, which is inspired by the behavior that is observed when analyzing the joint beamforming and jamming scheme. An assignment optimization problem is formulated for the ternary scheme, and this is based on the SINR metric in a similar way to the joint scheme. *Tabu search* (TS) is invoked to obtain the solution to the assignment problem.

The most important objective of PLS enhancement work is to increase the secrecy capacity [4]. However, in VLC systems, deriving a closed-form analytic expression for the secrecy capacity has proved elusive due to the amplitude constraint. Hence, upper and lower bounds for various channel models have been studied instead [9], [14], [29], [30]. Similarly, in this paper, by utilizing the truncated Gaussian distribution on the input and jamming signals as in [14], we derive a closed-form secrecy rate expression for the joint scheme, given the location of the eavesdropper. On the other hand, without knowledge of the location or the CSI of the eavesdropper, with only statistical information available, it is more appropriate

[1] We will provide an example for this situation in Section VI.

TABLE I. Notation and symbols used in the paper

Symbol	Definition/Explanation
L	the length of a room
W	the width of a room
H	the height from the ceiling to the work plane
N	number of transmitters
α	modulation index
I_{DC}	fixed bias current
ζ	current-to-light conversion efficiency
$\phi_{1/2}$	half illuminance angle
$A_{\mathrm{PD},k}$	physical area of a photodiode
$\phi_{i,k}$	angle of irradiance
$\psi_{i,k}$	angle of incidence
κ_k	refractive index of an optical concentrator
Ψ_k	received field of view of a photodiode
$R_{\mathrm{rsp.},k}$	photodetector's responsivity
T_k	transimpedance amplifier gain
$\mathbb{R}$	set of real numbers
$\mathbb{R}_+$	set of non-negative real numbers
$\mathbb{1}$	all-ones column vector
$\mathbb{0}$	all-zeros column vector
$\mathbf{I}$	identity matrix
$\mathbb{E}[\cdot]$	expectation operator
$[\cdot]^T$	transpose operator
$\mathbb{P}(\cdot)$	probability operator
$\mathbb{h}(\cdot)$	differential entropy operator
$\mathbb{I}(\cdot;\cdot)$	mutual information operator
$\lVert\cdot\rVert_1$	1-norm operator
$\log(\cdot)$	natural logarithm

to define and utilize the *average* secrecy rate as a metric to increase the secrecy performance [31], [32]. However, the expectation of the proposed secrecy rate cannot be written in closed-form, and the optimization problem maximizing the average secrecy rate is shown to be non-convex; thus, it is impractical to solve the problem directly, either by analytic or numerical means. Consequently, we propose a continuous LED model to mitigate the aforementioned complications and to solve the optimization problem numerically. We show that the continuum model can significantly simplify the optimization problem based on the average secrecy rate metric by transforming the problem with $2N$ optimization variables, where N is the number of LED transmitters, into a problem with only three optimization variables.

The rest of this paper is organized as follows[2]. Section II begins with the system model describing the data transmission and jamming schemes in VLC, and various performance measures are discussed. In Section III, the joint scheme based on the SINR is investigated. In Section IV, the ternary scheme is analyzed based on the SINR, and in Section V, the average secrecy rate under the ternary scheme is investigated by utilizing the continuum model. Section VI provides details of numerical results that support our analysis, and conclusions are drawn in Section VII.

II. System Model

A. Data Transmission and Jamming

We consider the downlink of a VLC system in a rectangular room as shown in Fig. 1, where W, L, and H denote the width, the length, and the height of the ceiling relative to the work plane, respectively. Also, one legitimate user R_U and one passive eavesdropper R_E are present in the room, where R_E is assumed to be randomly located on the work plane in the room. N LED transmitters are assumed to be attached to the ceiling of the room and each transmitter, i.e., an LED fixture consisting of multiple individual LEDs, is assumed to be capable of communicating independently of other transmitters. Moreover, throughout this paper, it is assumed that the transmitters know the location or the CSI of R_U, while not knowing those of R_E.

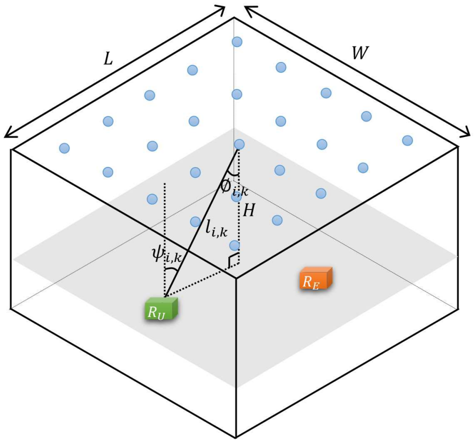


Fig. 1. Rectangular room configuration for VLC systems. W and L are the room's width and length, and H denotes the height from the ceiling to the work plane. Dots denote LED transmitters.

To enhance PLS in VLC systems, we employ a joint technique of beamforming and jamming. The data signal $x(t) \in [-1, 1]$ in time slot t is generated from a certain real constellation (e.g., a direct current (DC) biased pulse-amplitude modulation (PAM) VLC scheme) and multiplied by a beamforming weight ω_i ($|\omega_i| \le 1$) at the ith transmitter for $i \in \{1, 2, ..., N\}$ [20]. Also, the ith transmitter is assumed to be capable of independently transmitting a jamming signal $j_i(t) \in [-1, 1]$. Note that $j_i(t)$ must be a random value to prevent R_E from canceling the jamming component from the received signal. Therefore, the input signal $s_i(t)$ for the ith transmitter can be expressed as

$$s_i(t) = \alpha I_{DC} \left(\omega_i x(t) + \nu_i j_i(t)\right) \tag{1}$$

where $\alpha \in [0, 1]$ is termed the modulation index and $I_{DC} \in \mathbb{R}_+$ is a fixed bias current. The parameter ν_i ($\nu_i \ge 0$) is the jamming intensity for the ith transmitter, where $0 \le \nu_i + |\omega_i| \le 1$. The input signal $s_i(t)$ is superimposed on a fixed bias current I_{DC}, which is used for illumination. To maintain linear current-to-light conversion, the amplitude of $s_i(t)$ is constrained such that $|s_i(t)| \le \alpha I_{DC}$. Therefore, the dynamic range of the LED is $I_{DC} \pm \alpha I_{DC}$. Also, $\mathbb{E}[s_i(t)] = 0$ is assumed; thus the data and jamming signals do not affect illumination.

According to [33], the channel gain $h_{i,k} \in \mathbb{R}_+$ from the ith transmitter to the receiver R_k for $k \in \{U, E\}$ in a VLC system corresponding to an LED with a generalized Lambertian emission pattern is given by

$h_{i,k} =$

[2] The notation and symbols used in the paper are listed in Table I.

$$\begin{cases} \zeta \dfrac{(m+1)A_{\mathrm{PD},k}}{2\pi l_{i,k}^2} \dfrac{\kappa_k^2 \cos^m(\phi_{i,k})}{\sin^2(\Psi_k)} \cos(\psi_{i,k}) R_{\mathrm{rsp.},k} T_k & \text{for } |\psi_{i,k}| \leq \Psi_k, \\ 0 & \text{for } |\psi_{i,k}| > \Psi_k \end{cases} \tag{2}$$

where ζ is the current-to-light conversion efficiency and $m = -\ln(2)/\ln(\cos(\phi_{1/2}))$ is the order of Lambertian emission with half illuminance at $\phi_{1/2}$. $A_{\mathrm{PD},k}$ is the physical area of the PD of R_k. As shown in Fig. 1, $l_{i,k}$ is the distance between the ith transmitter and R_k. $\phi_{i,k}$ is the angle of irradiance and $\psi_{i,k}$ is the angle of incidence between the ith transmitter and R_k. Also, for R_k, κ_k is the refractive index of the optical concentrator, Ψ_k denotes the received field of view of the PD, $R_{\mathrm{rsp.},k}$ is the photodetector's responsivity, and T_k is the transimpedance amplifier gain.

Moreover, by assuming that a receiver's PD faces up normal to the work plane, we can rewrite (2) in terms of $l_{i,k}$ as

$$h_{i,k} = \zeta \frac{(m+1)A_{\mathrm{PD},k}}{2\pi l_{i,k}^2} \frac{\kappa_k^2}{\sin^2(\Psi_k)} \left(\frac{H}{l_{i,k}}\right)^{(m+1)} R_{\mathrm{rsp.},k} T_k = G_k l_{i,k}^{-(m+3)} \tag{3}$$

where $G_k = \zeta(m+1)A_{\mathrm{PD},k}\kappa_k^2 H^{m+1} R_{\mathrm{rsp.},k} T_k / 2\pi \sin^2(\Psi_k)$. Note that (3) is valid only when $|\psi_{i,k}| \leq \Psi_k$ is satisfied. Thus, for the sake of simplicity, we assume that all of the receivers are located such that $l_{i,k} \leq H/\cos(\Psi_k)$ is satisfied for all i.

Therefore, the received signal at R_k for $k \in \{U, E\}$ with the joint scheme of beamforming and jamming can be described as

$$y_k(t) = \alpha I_{DC} \mathbf{h_k^T} (\mathbf{w} x(t) + \mathbf{J} \mathbf{v}) + n_k(t) \tag{4}$$

where $\mathbf{h_k} = [h_{1,k}, h_{2,k}, ..., h_{N,k}]^T \in \mathbb{R}^N$ denotes the channel gain vector, and $\mathbf{w} = [\omega_1, \omega_2, ..., \omega_N]^T$ and $\mathbf{v} = [v_1, v_2, ..., v_N]^T$ denote the beamforming and jamming intensity vectors, respectively. Also, $\mathbf{J} = \mathrm{diag}(j_1(t), j_2(t), ..., j_N(t))$ is a diagonal jamming signal matrix, and $n_k(t)$ signifies zero-mean additive white Gaussian noise (AWGN) at R_k with variance σ^2. For notational convenience, the time index t is ignored for the remainder of the paper.

B. Performance Measures

For Gaussian VLC MISO channels with amplitude constraints, we define the peak SINR, rather than the average, by assuming $x = 1$ and $\mathbf{J} = \mathbf{I}$ since the channel capacity bounds of VLC systems are expressed as a function of the peak SINR [9], [10]. Therefore, the peak SINRs at R_U and R_E with the proposed joint technique can be written as

$$\gamma_U = \frac{\alpha^2 I_{DC}^2 \mathbf{w^T A w}}{\alpha^2 I_{DC}^2 \mathbf{v^T A v} + \sigma^2}, \tag{5a}$$

$$\gamma_E = \frac{\alpha^2 I_{DC}^2 \mathbf{w^T B w}}{\alpha^2 I_{DC}^2 \mathbf{v^T B v} + \sigma^2} \tag{5b}$$

respectively, where $\mathbf{A} = \mathbf{h_U h_U^T}$ and $\mathbf{B} = \mathbf{h_E h_E^T}$. We use SINR to denote the peak SINR for the remainder of the paper.

The secrecy capacity of the VLC channel is given by [4]

$$C_s = \max_{p_X} (\mathbb{I}(X; Y_U) - \mathbb{I}(X; Y_E)), \tag{6a}$$

$$\text{s.t.} \quad |x| \leq 1 \tag{6b}$$

where X denotes the transmitted optical signal and p_X is the input distribution of X. Also, Y_k for $k \in \{U, E\}$ denotes the signal observed by the receiver R_k. The relationship between X and Y_k can be written as $Y_k = H_k X + N_k$, where H_k is the channel gain between the transmitter and R_k. N_k is noise at R_k. It is not feasible to deduce a closed-form solution for (6) due to the amplitude constraint [34]. It was shown in [34], [35] that the optimal probability distribution p_X, i.e., the solution of the optimization problem (6), is unique and discrete with a finite support set, thus it can be efficiently solved using numerical methods. Nevertheless, closed-form expressions are often preferred for engineering systems. In the following, we provide a closed-form expression for an achievable secrecy rate with the joint scheme of beamforming and jamming.

Firstly, to simplify the wiretap channel model in (4), we assume that the jammers emit an identical jamming signal, i.e., $\mathbf{J} = j \cdot \mathbf{I}$, where j is a (random) jamming signal. This simplification might weaken the security, but it may be preferred since it permits a simple implementation. In addition, to simplify deriving a closed-form achievable secrecy rate expression, we assume that both the data signal x and the jamming signal j follow the truncated Gaussian distribution $\mathcal{N}_T(0, \sigma_T^2)$ defined over $[-1, 1]$ as in [14]. Its probability density function (PDF) is given by

$$f(x) = \frac{\phi\left(\frac{x}{\sigma_T}\right)}{\Phi\left(\frac{1}{\sigma_T}\right) - \Phi\left(\frac{-1}{\sigma_T}\right)} \tag{7}$$

where $\phi(\upsilon) = e^{-\upsilon^2/2}/\sqrt{2\pi}$, $\Phi(\tau) = (1 + \mathrm{erf}(\tau/\sqrt{2}))/2$ and $\sigma_T \in \mathbb{R}_+$. Note that the optimal input distribution under the amplitude constraint in VLC systems is not readily available, and the truncated Gaussian distribution was shown to outperform the uniform distribution in the terms of secrecy rates in VLC systems [14]. Therefore, from (4), the received signals for R_U and R_E with these simplifications can be rewritten as

$$y_U = \alpha I_{DC} \mathbf{h_U^T w} x + \alpha I_{DC} \mathbf{h_U^T v} j + n_U, \tag{8a}$$

$$y_E = \alpha I_{DC} \mathbf{h_E^T w} x + \alpha I_{DC} \mathbf{h_E^T v} j + n_E \tag{8b}$$

respectively. We now present the following lemma, which captures an analytic achievable secrecy rate expression for the system in question.

Lemma 1. *An achievable secrecy rate for the Gaussian wiretap channel in (8) with the joint technique of beamforming and jamming can be obtained by lower-bounding the secrecy capacity in (6) to give*

$$R_s = \max \left\{ \frac{1}{2} \log \left(\frac{e^{2\eta} \left(\mathbf{w^T A w} + \mathbf{v^T A v} \right) + C}{\varphi \mathbf{v^T A v} + C} \right) - \frac{1}{2} \log \left(\frac{\varphi \left(\mathbf{w^T B w} + \mathbf{v^T B v} \right)}{e^{2\eta} \mathbf{v^T B v}} \right), 0 \right\} \tag{9}$$

where

$$\eta = \log(Z) + \frac{-\frac{1}{\sigma_T} \phi\left(\frac{-1}{\sigma_T}\right) - \frac{1}{\sigma_T} \phi\left(\frac{1}{\sigma_T}\right)}{2Z},$$

$$\varphi = 1 + \frac{\frac{-1}{\sigma_T}\phi\left(\frac{-1}{\sigma_T}\right) - \frac{1}{\sigma_T}\phi\left(\frac{1}{\sigma_T}\right)}{Z} - \left(\frac{\phi\left(\frac{-1}{\sigma_T}\right) - \phi\left(\frac{1}{\sigma_T}\right)}{Z}\right)^2,$$

$$Z = \Phi\left(\frac{1}{\sigma_T}\right) - \Phi\left(\frac{-1}{\sigma_T}\right),$$

$$C = \frac{\sigma^2}{\alpha^2 I_{DC}^2 \sigma_T^2}.$$

Proof. See Appendix A-A. □

III. The Joint Strategy of Beamforming and Jamming

A. Optimization of the Joint Strategy Based on SINR

Without knowledge of the location or the CSI of R_E, a natural objective is to maximize the SINR of R_U subject to a constraint on the *average* SINR of R_E, same as in RF communications [36], [37]. Therefore, in this subsection, we investigate the selection of $\mathbf{w}$ and $\mathbf{v}$ that maximizes γ_U subject to a constraint on $\mathbb{E}_{\mathbf{h_E}}[\gamma_E]$.

From the SINR definitions of (5), we can formulate the problem of interest as

$$\arg\max_{\mathbf{w},\mathbf{v}} \frac{\alpha^2 I_{DC}^2 \mathbf{w^T A w}}{\alpha^2 I_{DC}^2 \mathbf{v^T A v} + \sigma^2} \tag{10a}$$

$$\text{s.t.} \begin{cases} \mathbb{E}_{\mathbf{h_E}}\left[\frac{\alpha^2 I_{DC}^2 \mathbf{w^T B w}}{\alpha^2 I_{DC}^2 \mathbf{v^T B v} + \sigma^2}\right] \le \rho_E \\ |\mathbf{w}| + \mathbf{v} \preceq \mathbb{1} \\ \mathbf{v} \succeq \mathbb{0}. \end{cases} \tag{10b}$$

where ρ_E is the target constraint on $\mathbb{E}_{\mathbf{h_E}}[\gamma_E]$. However, due to the fact that the first constraint does not lead to a tractable analysis, we propose a suboptimal approach by replacing the left term of the first constraint with the ratio of the average received data power to the average interference plus noise power[3], i.e.,

$$\overline{\gamma}_E \coloneqq \frac{\mathbb{E}_{\mathbf{h_E}}\left[\alpha^2 I_{DC}^2 \mathbf{w^T B w}\right]}{\mathbb{E}_{\mathbf{h_E}}\left[\alpha^2 I_{DC}^2 \mathbf{v^T B v} + \sigma^2\right]} = \frac{\alpha^2 I_{DC}^2 \mathbf{w^T \overline{B} w}}{\alpha^2 I_{DC}^2 \mathbf{v^T \overline{B} v} + \sigma^2} \tag{11}$$

where $\overline{\mathbf{B}} = \mathbb{E}_{\mathbf{h_E}}[\mathbf{h_E h_E^T}]$. The element in the ith row and jth column of $\overline{\mathbf{B}}$ is given by

$$\overline{B}_{i,j} = \frac{1}{L \cdot W}\int_{\frac{-L}{2}}^{\frac{L}{2}}\int_{\frac{-W}{2}}^{\frac{W}{2}} \frac{G_E^2}{l_i^{m+3}(x,y) l_j^{m+3}(x,y)}\,\mathrm{d}x\,\mathrm{d}y \tag{12}$$

where $l_i(x,y)$ for $i \in \{1, 2, \cdots, N\}$ is the distance between the ith transmitter and the point (x,y) in the work plane.

Now, we consider the optimization problem given by

$$\arg\max_{\mathbf{w},\mathbf{v}} \frac{\alpha^2 I_{DC}^2 \mathbf{w^T A w}}{\alpha^2 I_{DC}^2 \mathbf{v^T A v} + \sigma^2} \tag{13a}$$

$$\text{s.t.} \begin{cases} \frac{\alpha^2 I_{DC}^2 \mathbf{w^T \overline{B} w}}{\alpha^2 I_{DC}^2 \mathbf{v^T \overline{B} v} + \sigma^2} \le \overline{\rho}_E \\ |\mathbf{w}| + \mathbf{v} \preceq \mathbb{1} \\ \mathbf{v} \succeq \mathbb{0}. \end{cases} \tag{13b}$$

where $\overline{\rho}_E$ is the target constraint on $\overline{\gamma}_E$. Utilizing the Charnes-Cooper transformation [38], we can simplify the objective function (13a). First, we define

$$\mathbf{w} = \frac{\tilde{\mathbf{w}}}{\xi},\ \mathbf{v} = \frac{\tilde{\mathbf{v}}}{\xi} \tag{14}$$

where $\xi > 0$. Then, by plugging (14) into (13) and setting $\xi = \sqrt{1 - \alpha^2 I_{DC}^2 \tilde{\mathbf{v}}^\mathbf{T} \mathbf{A} \tilde{\mathbf{v}}}/\sigma$, the quadratic fractional optimization problem (13) can be simplified to the non-fractional problem

$$\arg\max_{\tilde{\mathbf{w}},\tilde{\mathbf{v}}} \alpha^2 I_{DC}^2 \tilde{\mathbf{w}}^\mathbf{T} \mathbf{A} \tilde{\mathbf{w}} \tag{15a}$$

$$\text{s.t.} \begin{cases} \alpha^2 I_{DC}^2 \tilde{\mathbf{w}}^\mathbf{T} \overline{\mathbf{B}} \tilde{\mathbf{w}} - \overline{\rho}_E + \rho_E \alpha^2 I_{DC}^2 \tilde{\mathbf{v}}^\mathbf{T} \mathbf{A} \tilde{\mathbf{v}} \le \overline{\rho}_E \alpha^2 I_{DC}^2 \tilde{\mathbf{v}}^\mathbf{T} \overline{\mathbf{B}} \tilde{\mathbf{v}} \\ |\tilde{\mathbf{w}}| + \tilde{\mathbf{v}} \preceq \mathbb{1} \cdot \sqrt{1 - \alpha^2 I_{DC}^2 \tilde{\mathbf{v}}^\mathbf{T} \mathbf{A} \tilde{\mathbf{v}}}/\sigma \\ \tilde{\mathbf{v}} \succeq \mathbb{0}. \end{cases} \tag{15b}$$

Here, the difficulty of solving (15) arises from the fact that it requires the maximization of a convex quadratic objective function and the right side of the first constraint yields a non-convex set. Thus, we apply the CCP approach, which is a powerful heuristic method to find a local solution. Given initial feasible points $\tilde{\mathbf{w}}_0$ and $\tilde{\mathbf{v}}_0$, we transform the objective function and the non-convex function in the first constraint into affine functions (i.e., convex) by calculating the first-order Taylor series approximation. We then solve the convex optimization problem by using a standard optimization programming like the sequential quadratic programming (SQP) algorithm [39]. Next, we set the solution to $\tilde{\mathbf{w}}_1$ and $\tilde{\mathbf{v}}_1$ and repeat the same procedure until the improvement in the objective value is less than a predefined threshold ϵ. The details of this iterative algorithm are given in Algorithm 1. Since the CCP is a local heuristic, the final solution depends on the initial points $\tilde{\mathbf{w}}_0$ and $\tilde{\mathbf{v}}_0$. Therefore, it is wise to start the algorithm with several initial points and take as the final choice denoted by $\tilde{\mathbf{w}}^*$ and $\tilde{\mathbf{v}}^*$ which maximizes the objective function. On the other hand, it is worth noting that the initial points can be somewhat anticipated according to the location of R_U, since it is expected that the beamforming weights are relatively high for the transmitters that are near to R_U, while the jamming intensities are relatively high for the transmitters that are far away from R_U.

Finally, from (14), we can obtain the optimal solution to the original problem in (13) by computing

$$\mathbf{w}^* = \frac{\sigma \tilde{\mathbf{w}^*}}{\sqrt{1 - \alpha^2 I_{DC}^2 \tilde{\mathbf{v}^*}^T \mathbf{A} \tilde{\mathbf{v}^*}}},\ \mathbf{v}^* = \frac{\sigma \tilde{\mathbf{v}^*}}{\sqrt{1 - \alpha^2 I_{DC}^2 \tilde{\mathbf{v}^*}^T \mathbf{A} \tilde{\mathbf{v}^*}}}. \tag{16}$$

[3] Note that $\overline{\gamma}_E$ does not approximate to the expectation of γ_E, i.e., $\mathbb{E}_{\mathbf{h_E}}[\gamma_E]$. For example, when 6×6 LEDs and a room of 30×30 m^2 are assumed, $\overline{\gamma}_E = 0.07$ and $\mathbb{E}_{\mathbf{h_E}}[\gamma_E] = 3.17$ are numerically evaluated. However, as we will see in the following, $\overline{\gamma}_E$ is a very effective metric for suppressing the information reception and increasing the interference at R_E, while significantly simplifying the optimization problem.

Algorithm 1 CCP algorithms for solving (15)

```
given initial feasible points $\tilde{\mathbf{w}}_0$ and $\tilde{\mathbf{v}}_0$, $k := 0$
repeat
    1. Convexify. Form
    $g_0(\tilde{\mathbf{w}};\tilde{\mathbf{w}}_k) \triangleq \alpha^2 I_{DC}^2 \tilde{\mathbf{w}}_k^{\mathrm{T}}\mathbf{A}\tilde{\mathbf{w}}_k + 2(\alpha^2 I_{DC}^2\mathbf{A}\tilde{\mathbf{w}}_k)^T(\tilde{\mathbf{w}}-\tilde{\mathbf{w}}_k)$,
    $g_1(\tilde{\mathbf{v}};\tilde{\mathbf{v}}_k) \triangleq \overline{\rho}_E\alpha^2 I_{DC}^2 \tilde{\mathbf{v}}_k^{\mathrm{T}}\overline{\mathbf{B}}\tilde{\mathbf{v}}_k + 2\overline{\rho}_E(\alpha^2 I_{DC}^2\overline{\mathbf{B}}\tilde{\mathbf{v}}_k)^T(\tilde{\mathbf{v}}-\tilde{\mathbf{v}}_k)$
    2. Solve. Set the value of $\tilde{\mathbf{w}}_{k+1}$ and $\tilde{\mathbf{v}}_{k+1}$ to solutions of the convex problem
    $\arg\max_{\tilde{\mathbf{w}},\tilde{\mathbf{v}}} \; g_0(\tilde{\mathbf{w}};\tilde{\mathbf{w}}_k)$
    $\text{s.t.} \begin{cases} \alpha^2 I_{DC}^2\tilde{\mathbf{w}}^{\mathbf{T}}\overline{\mathbf{B}}\tilde{\mathbf{w}} - \overline{\rho}_E + \rho_E\alpha^2 I_{DC}^2\tilde{\mathbf{v}}^{\mathbf{T}}\mathbf{A}\tilde{\mathbf{v}} \le g_1(\tilde{\mathbf{v}};\tilde{\mathbf{v}}_k) \\ |\tilde{\mathbf{w}}| + \tilde{\mathbf{v}} \le \mathbb{1}\cdot\frac{\sqrt{1-\alpha^2 I_{DC}^2\tilde{\mathbf{v}}^T\mathbf{A}\tilde{\mathbf{v}}}}{\sigma} \\ \tilde{\mathbf{v}} \ge \mathbb{0} \end{cases}$
    3. Update iteration. $k := k + 1$.
until stopping criterion is satisfied.
```

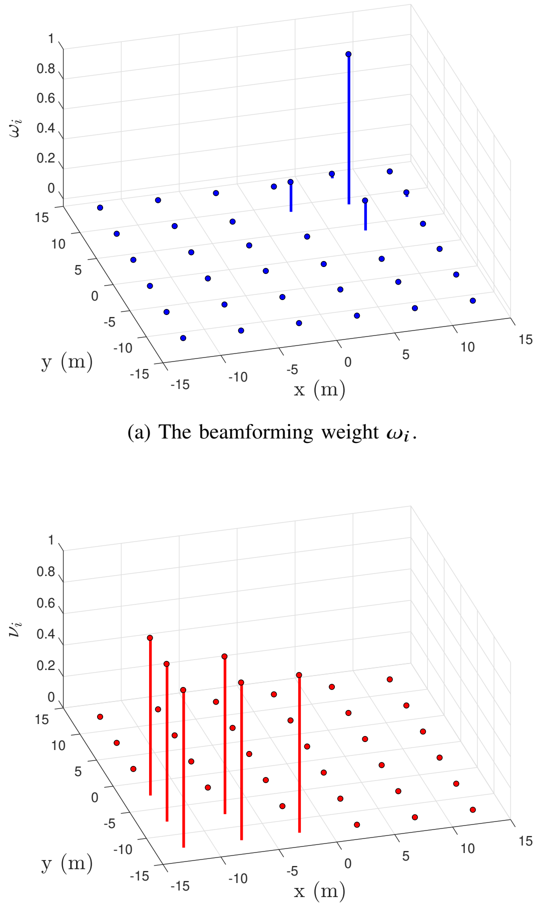
B. Beamforming and Jamming Characteristics

In the previous section, we showed that the beamforming weight and jamming intensity vectors of the optimization problem (13), which is based on the SINR, can be effectively found by utilizing the Charnes-Cooper transformation and the CCP. However, this approach suffers from considerable computational overhead as well as a large number of iterations when the number of LED transmitters is large. Because, as we will see later, the joint scheme will be more useful in a huge room consisting of a large number of transmitters, the complexity in finding the beamforming and jamming vectors must be reduced. Therefore, in this subsection, we investigate the characteristics of the beamforming weights and jamming intensities according to the relative locations among the transmitters and R_U. This investigation will enable us to propose a simple ternary scheme in the next section.

Figs. 2(a) and (b) show an example of the beamforming weights and the jamming intensities of the transmitters according to the locations of the transmitters, which are obtained by solving (13). We assume that 6×6 transmitters are located at (x_T, y_T, H) for $x_T, y_T \in \{\pm 2.5, \pm 7.5, \pm 12.5\}$. Also, we assume that one fixed R_U is located at $(7, 7, 0)$ and one R_E is randomly located in the work plane of the room. It is shown that the beamforming weights of the transmitters being located near to R_U are high, while those of the other transmitters are almost zero. In contrast, the jamming intensities of the transmitters being located near to R_U are zero, while those of other transmitters are close to one. Thus, this result verifies that when the transmitters do not retain the information on the location or the CSI of an eavesdropper, transmitting data only by the transmitters being located near to the legitimate user and emitting jamming signals by the faraway transmitters would effectively increase the secrecy performance. In other words, simultaneously transmitting information and jamming signals from the same transmitter would be unusual.

IV. The Ternary Strategy Based on SINR

As a result of the observations noted in Section III-B, we propose a simple ternary strategy in which the transmitter selects its role among an information transmitter, a jammer or just being silent. In other words, when the transmitter acts as the information transmitter, their beamforming weights are always one, while their jamming intensities are always zero. For jammers, the situation is reversed. Also, a transmitter can remain silent if need be. The ternary scheme can significantly reduce the computational complexity since the transmitters only need to select one role out of the three options based on the location of R_U.



(a) The beamforming weight ω_i.

(b) The jamming intensity ν_i.

Fig. 2. The beamforming and jamming vectors obtained from the optimization problem (13). R_U is located at $(7, 7, 0)$. The 6×6 LED transmitters are located at (x_T, y_T, H) for $x_T, y_T \in \{\pm 2.5, \pm 7.5, \pm 12.5\}$. $L = 30$ m, $W = 30$ m, $H = 2.2$ m, $\phi_{1/2} = 60°$ and $\overline{\rho}_E = 0.15$ are used.

In the proposed scheme, the beamforming weights ω_i and the jamming intensities ν_i for all $i \in \{1, 2, ..., N\}$ have to be an element of $\{0, 1\}$, subject to $w_i + \nu_i \le 1$. We will investigate the assignment optimization problem for the ternary strategy based on the SINR metric, which can be effectively solved by TS.

The optimization problem for the joint scheme based on the SINR (13) can be modified under the ternary strategy as

$$\arg\max_{\mathbf{w},\mathbf{v}} \; \frac{\alpha^2 I_{DC}^2\mathbf{w}^{\mathbf{T}}\mathbf{A}\mathbf{w}}{\alpha^2 I_{DC}^2\mathbf{v}^{\mathbf{T}}\mathbf{A}\mathbf{v} + \sigma^2} \tag{17a}$$

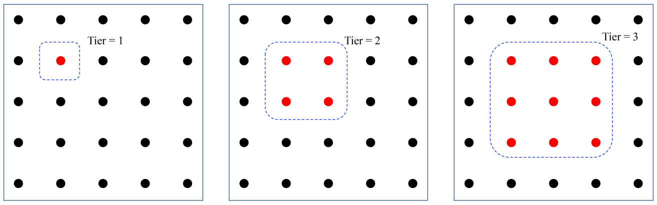


Fig. 3. Examples of tier groups. The move of the TS changes the roles of transmitters in a tier group.

$$\text{s. t.} \begin{cases} \dfrac{\alpha^2 I_{DC}^2 \mathbf{w}^{\mathbf{T}}\overline{\mathbf{B}}\mathbf{w}}{\alpha^2 I_{DC}^2 \mathbf{v}^{\mathbf{T}}\overline{\mathbf{B}}\mathbf{v} + \sigma^2} \leq \overline{\rho}_E \\ |\mathbf{w}| + \mathbf{v} \preceq \mathbb{1} \\ \omega_i,\ v_i \in \{0,1\} \quad \text{for all } i \in \{1,2,\ldots,N\}. \end{cases} \tag{17b}$$

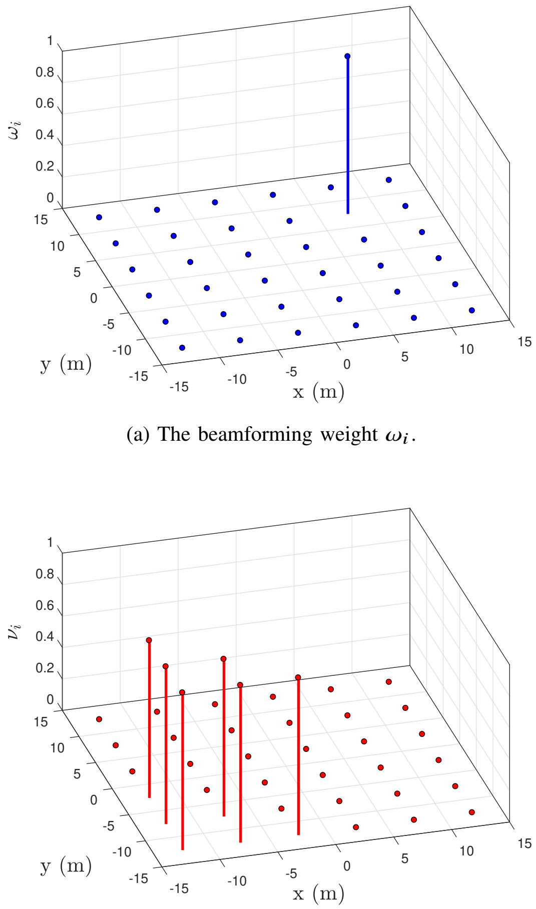
A fractional quadratic assignment optimization problem like (17) was shown as NP-hard [40]; thus, it would not be feasible to find an optimal point of (17) via a deterministic method. Therefore, we employ TS [41], which is a meta-heuristic method utilizing local search procedures, to find the local optimal solutions $\mathbf{w}^*$ and $\mathbf{v}^*$ of (17). TS is designed to prevent a search procedure from becoming trapped at locally optimal solutions by utilizing short-term memory.

The TS procedure begins with the initial point $\{\mathbf{w}^*_{(0)}, \mathbf{v}^*_{(0)}\}$ in which the transmitters near to R_U are set as information transmitters, i.e., $\omega_i = 1$, while the others are set as jammers, i.e., $v_i = 1$. Setting the initial point in this way comes from the observation in Section III-B that the transmitters near to R_U are likely to act as information transmitters, while the distant transmitters are likely to act as jammers.

Then, a set of neighboring solutions $N(\{\mathbf{w}^*_{(0)}, \mathbf{v}^*_{(0)}\})$ are generated by applying a set of possible *moves* to $\{\mathbf{w}^*_{(0)}, \mathbf{v}^*_{(0)}\}$. The set of possible moves includes "set information transmitters", "set jammers", "set silent transmitters" and "swap roles". Since the roles of the transmitters largely depend on their locations with respect to R_U, it can be anticipated that the roles of the transmitters being located near to each other would be identical. Thus, we enable the moves to change the roles of the transmitters in a tier group as shown in Fig. 3. With these grouping moves, we can reduce the possibility that the search procedure is trapped at a local solution. Note that the efficiency and performance of a TS procedure strongly depend on the way that the moves are defined and how well the moves exploit the actual structure of the problem [41].

Next, among the neighborhood solutions $N(\{\mathbf{w}^*_{(0)}, \mathbf{v}^*_{(0)}\})$, the best solution in the terms of maximizing the objective function is selected as the iterate $\{\mathbf{w}^*_{(1)}, \mathbf{v}^*_{(1)}\}$ even if the value of the objective function with $\{\mathbf{w}^*_{(1)}, \mathbf{v}^*_{(1)}\}$ is less than the value with $\{\mathbf{w}^*_{(0)}, \mathbf{v}^*_{(0)}\}$. Also, in order to prevent cycling and to try to escape from local optima, the list of tabu moves is maintained. This list forbids the opposite move that has been made at a given step for a certain number of iterations L, which is the length of the tabu list. In addition, if the move added to the tabu list yields an improved solution larger than "aspiration criteria", the move can be made, and its solution can be selected as the best solution for the next iteration.

This procedure repeats for a maximum number of iterations max_{it}. At each iteration, the best solution $\{\mathbf{w}^*_{(i)}, \mathbf{v}^*_{(i)}\}$ and its value of the objective function are stored, and the best solution among them is returned as the final optimal solution.



(a) The beamforming weight ω_i.

(b) The jamming intensity v_i.

Fig. 4. The beamforming and jamming vectors with the ternary scheme obtained from the assignment optimization problem (17). R_U is located at $(7,7,0)$. The 6×6 LED transmitters are located at (x_T, y_T, H) for $x_T, y_T \in \{\pm 2.5, \pm 7.5, \pm 12.5\}$. $L = 30$ m, $W = 30$ m, $H = 2.2$ m, $\phi_{1/2} = 60°$ and $\overline{\rho}_E = 0.15$ are used.

Fig. 4 shows the beamforming weights and jamming intensities found via TS under the ternary scheme. It is shown that they are similar to the result in Fig. 2, except that the values of beamforming weights and jamming intensities are either 1 or 0. Note that on a standard PC (Intel i7, 3.4 GHz) using MATLAB, finding a solution via TS can be executed in a few seconds, while the CCP for solving (13) requires hundreds of seconds, including the time for iterations with multiple different initial points, when $N = 36$.

V. Optimization Based on Secrecy Rate with the Continuum Model

In this section, we consider a continuum model of the system in an effort to investigate the average secrecy rate with the ternary scheme. Note that, to the best of our knowledge, with the discrete transmitter model described in Fig. 1, it is only possible to solve the maximum-SINR problem; a solution to the maximum-average-secrecy-rate problem remains elusive.

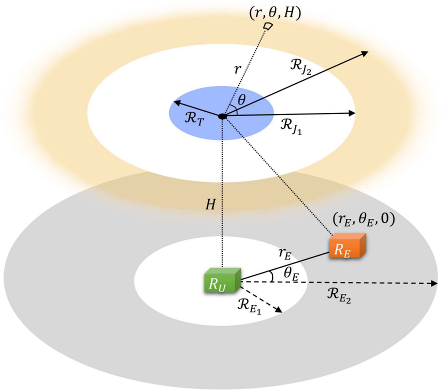


Fig. 5. Geometry of the ternary scheme with the continuous LED model.

This is due to the fact that the optimization problem is not convex in the $2N$ variables (where N can be large) to be optimized. Furthermore, $\mathbb{E}_{\mathbf{h_E}}[R_s]$ is difficult to evaluate owing to the terms $\mathbf{w^T Bw}$ and $\mathbf{v^T Bv}$, where each element of $\mathbf{B}$ is a function of $h_{i,E}$. However, by utilizing the continuum model, we can make the optimization problem simple enough to be numerically analyzed as we will see below.

Fig. 5 illustrates the geometry of the continuum model, where an infinite number of LEDs are assumed to be attached to the ceiling in an infinitely large room, and their distances among LEDs are infinitesimal. In practice, a lot of multiple LEDs are uniformly and widely distributed to evenly illuminate an entire room within the lighting standards, e.g., from 400 to 1000 lux for a typical office [42]. Thus, the continuum model can describe practical VLC systems and is able to provide analytic insight into the secrecy performance of the ternary strategy. Without loss of generality, we assume that R_U is located at the origin and R_E is located in a gray annulus with inner radius $\mathcal{R}_{E_1}$ and outer radius $\mathcal{R}_{E_2}$[4]. The blue shaded circular plane centered at R_U denotes the LEDs that act as the information transmitters, while the yellow annulus with inner radius $\mathcal{R}_{J_1}$ and outer radius $\mathcal{R}_{J_2}$ denotes the jammers. The white annulus indicates the LEDs that are silent.

A. Received Optical Power Density Analysis

In the continuum model, to deal with the infinite number of LEDs, we characterize the emitted optical power of LEDs by the optical power density per unit of LED area P_T [W/m^2]. We assume that the information transmitter and the jammer emit signals with the same optical power density.

Firstly, the received optical power density of the data signal emitted by the information transmitters, i.e., the blue shaded plane, P_D [W/m^2] at $(r_E, \theta_E, 0)$ can be described by

$$P_D(r_E,\theta_E) = \int_0^{\mathcal{R}_T}\int_0^{2\pi} P_T \frac{(m+1)}{2\pi l_E^2}\left(\frac{H}{l_E}\right)^{(m+1)} r\,\mathrm{d}\theta\,\mathrm{d}r$$

$$\overset{(a)}{=} \frac{P_T}{2}\left(1+\frac{\mathcal{R}_T^2-H^2-r_E^2}{\sqrt{(H^2+\mathcal{R}_T^2)^2+2r_E^2(H^2-\mathcal{R}_T^2)+r_E^4}}\right) \tag{18}$$

where $l_E = \sqrt{r^2 + r_E^2 - 2rr_E\cos(\theta-\theta_E) + H^2}$ is the distance between the differential transmitter and the point $(r_E, \theta_E, 0)$. Also, for (a) and the following analysis, we assume all of the LED transmitters have the *Lambertian* emission pattern, i.e., $\phi_{1/2} = 60^\circ$ $(m = 1)$. Note that the value of $P_D(r_E, \theta_E)$ is independent of θ_E; thus we replace the notation of $P_D(r_E, \theta_E)$ with $P_D(r_E)$.

In addition, the received optical power density of the jamming signal emitted by the jammers, i.e., the yellow annulus, P_J [W/m^2] at $(r_E, \theta_E, 0)$ can be described as (19) at the top of the next page. Similarly, we replace the notation of $P_J(r_E, \theta_E)$ with $P_J(r_E)$.

B. SINR and Secrecy Rate Analysis

With the same simplifications assumed in (8), the received signals for R_U at the origin and R_E at $(r_E, \theta_E, 0)$ with the ternary scheme can be rewritten as

$$y_U(t) = \zeta_U P_D(0)x + \zeta_U P_J(0)j + n_U, \tag{20a}$$

$$y_E(t) = \zeta_E P_D(r_E)x + \zeta_E P_J(r_E)j + n_E \tag{20b}$$

respectively, where $\zeta_k = \alpha A_{\mathrm{PD},k}\kappa_k^2 R_{\mathrm{rsp.},k}T_k/\sin^2(\Psi_k)$ for $k \in \{U, E\}$. Also, the secrecy rate expression under the ternary scheme in (9) can be rewritten with the continuum model as

$$R_{s,\mathrm{cont.}}(r_E) = \max\left\{\frac{1}{2}\log\left(\frac{e^{2\eta}(P_D^2(0)+P_J^2(0))+D}{\varphi P_J^2(0)+D}\right)\right.$$
$$\left.-\frac{1}{2}\log\left(\frac{\varphi(P_D^2(r_E)+P_J^2(r_E))}{e^{2\eta}P_J^2(r_E)}\right), 0\right\} \tag{21}$$

where $D = \sigma^2/\sigma_T^2\zeta_U^2$.

C. Optimization Based on Average Secrecy Rate

Since the location of the eavesdropper is unknown at the transmitters, with only its statistical information being available, we can numerically calculate the *average* secrecy rate as

$$\overline{R}_{s,\mathrm{cont.}} = \int_{\mathcal{R}_{E_1}}^{\mathcal{R}_{E_2}} f_{r_E}(r)R_{s,\mathrm{cont.}}(r)\,\mathrm{d}r$$
$$= \int_{\mathcal{R}_{E_1}}^{\mathcal{R}_{E_2}} \frac{2r}{\mathcal{R}_{E_2}^2-\mathcal{R}_{E_1}^2}R_{s,\mathrm{cont.}}(r)\,\mathrm{d}r \tag{22}$$

where $f_{r_E}(r) = 2r/(\mathcal{R}_{E_2}^2 - \mathcal{R}_{E_1}^2)$ denotes the PDF of r_E. The problem of maximizing the average secrecy rate (23) can be formulated as

$$\overline{R}^\star_{s,\mathrm{cont.}} = \max_{\mathcal{R}_T,\mathcal{R}_{J_1},\mathcal{R}_{J_2}} \overline{R}_{s,\mathrm{cont.}} \tag{23}$$
$$\text{s.t.}\quad 0 \le \mathcal{R}_T \le \mathcal{R}_{J_1} \le \mathcal{R}_{J_2}.$$

Note that the optimization problem (23) is also a non-convex problem, and the objective function includes the integration to be solved numerically. However, the continuum model

[4] This assumption can be justified since R_E would like to be located not too near to R_U to escape the vigilance of a legitimate user and not too far from R_U to wiretap the information signal.

$$
\begin{aligned}
P_J(r_E,\theta_E) &= \int_{\mathcal{R}_{J_1}}^{\mathcal{R}_{J_2}} \int_0^{2\pi} P_T \frac{(m+1)}{2\pi l_E^2} \left(\frac{H}{l_E}\right)^{(m+1)} r \,\mathrm{d}\theta \,\mathrm{d}r \\
&= \frac{P_T}{2} \left(\frac{H^2 - \mathcal{R}_{J_1}^2 + r_E^2}{\sqrt{H^4 + \left(\mathcal{R}_{J_1}^2 - r_E^2\right)^2 + 2H^2\left(\mathcal{R}_{J_1}^2 + r_E^2\right)}} - \frac{H^2 - \mathcal{R}_{J_2}^2 + r_E^2}{\sqrt{H^4 + \left(\mathcal{R}_{J_2}^2 - r_E^2\right)^2 + 2H^2\left(\mathcal{R}_{J_2}^2 + r_E^2\right)}} \right)
\end{aligned}
\tag{19}
$$

significantly reduces the problem from finding the optimal beamforming and jamming vectors consisting of $2N$ elements in the discrete model to finding only three variables, i.e., $\mathcal{R}_T$, $\mathcal{R}_{J_1}$ and $\mathcal{R}_{J_2}$. Moreover, $\overline{R}^{\star}_{s,\text{cont.}}$ includes only a one-dimensional integral. In practice, finding the optimal solutions of the three parameters via the SQP algorithm can be executed in a second on a standard PC (Intel i7, 3.4 GHz) using MATLAB.

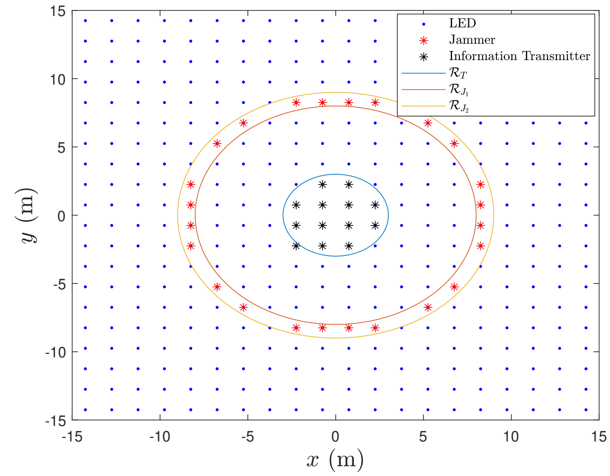


Fig. 6. An example of the role selection of the discrete transmitters. For the continuum model, $\mathcal{R}_T = 3$ m, $\mathcal{R}_{J_1} = 8$ m and $\mathcal{R}_{J_2} = 9$ m are assumed. For the discrete model, the 20×20 discrete LED transmitters are assumed to be uniformly distributed on a square lattice in the 30×30 m^2 room.

D. Link Between the Continuum and Discrete Cases

In this subsection, we provide guidelines on how to apply the three parameters $\mathcal{R}_T$, $\mathcal{R}_{J_1}$ and $\mathcal{R}_{J_2}$ obtained from the continuum model to a real VLC system, that is, the discrete model. To transform the continuous model to the discrete model in a straightforward manner, we set the roles of the discrete transmitters in minimizing the sum of the distances between the continuous and discrete transmitters. More specifically, assuming that R_U is located at the origin of our coordinate system and N LED transmitters are uniformly distributed over the entire room, selecting the jammers is executed as

$$
\begin{aligned}
\mathcal{J}^* = \min_{\mathcal{J}} & \sum_{i\in\mathcal{J}} d_{J,i} \\
\text{s.t.}\ & |\mathcal{J}| = N_J
\end{aligned}
\tag{24}
$$

where $N_J = \pi(\mathcal{R}_{J_2}^2 - \mathcal{R}_{J_1}^2)P_T/(I_{DC}\zeta)$ denotes the number of the jammers and $\mathcal{J} = \{j_1, j_2, \ldots, j_{N_J}\}$ for $j_i \in \{1,2,\ldots,N\}$ denotes the index set of the jammers. Also, $d_{J,i}$ denotes the shortest distances between the discrete transmitters and the continuous set of the jammers, which can be defined as

$$
d_{J,i} = \begin{cases}
\mathcal{R}_{J_1} - \sqrt{x_i^2 + y_i^2} & \text{for} \quad 0 \le \sqrt{x_i^2 + y_i^2} < \mathcal{R}_{J_1}, \\
0 & \text{for} \quad \mathcal{R}_{J_1} \le \sqrt{x_i^2 + y_i^2} < \mathcal{R}_{J_2}, \\
\sqrt{x_i^2 + y_i^2} - \mathcal{R}_{J_2} & \text{for} \quad \mathcal{R}_{J_2} \le \sqrt{x_i^2 + y_i^2}
\end{cases}
\tag{25}
$$

where $\{x_i, y_i\}$ for $i \in \{1,2,\ldots,N\}$ denotes the coordinates of the transmitters.

In addition, selecting the information transmitters can be similarly executed as

$$
\begin{aligned}
\mathcal{T}^* = \min_{\mathcal{T}} & \sum_{i\in\mathcal{T}} d_{T,i} \\
\text{s.t.}\ & |\mathcal{T}| = N_T
\end{aligned}
\tag{26}
$$

where $N_T = \pi\mathcal{R}_T^2 P_T/(I_{DC}\zeta)$ denotes the number of the information transmitters and $\mathcal{T} = \{t_1, t_2, \ldots, t_{N_T}\}$ for $t_i \in \{1,2,\ldots,N\}$ denotes the index set of the transmitters. $d_{T,i}$ denotes the shortest distances between the discrete transmitters and the continuous set of transmitters, which can be defined as

$$
d_{T,i} = \begin{cases}
0 & \text{for} \quad 0 \le \sqrt{x_i^2 + y_i^2} < \mathcal{R}_T, \\
\sqrt{x_i^2 + y_i^2} - \mathcal{R}_T & \text{for} \quad \mathcal{R}_T \le \sqrt{x_i^2 + y_i^2}.
\end{cases}
\tag{27}
$$

Fig. 6 shows an example of mapping the continuous transmitter to the discrete transmitters minimizing the sum of the distances, where the 20×20 LEDs are distributed on a square lattice.

Once the mapping is finalized, the secrecy rate with the selected discrete information transmitters and jammers given the R_E location, whose coordinate in the work plane is (r_E, θ_E), can be calculated as

$$
\begin{aligned}
R_{s,\text{disc.}}(r_E,\theta_E) = \max \Bigg\{ & \frac{1}{2}\log\left(\frac{e^{2\eta}\left(\mathbf{e}_\mathbf{T}^\mathbf{T}\mathbf{A}\mathbf{e}_\mathbf{T} + \mathbf{e}_\mathbf{J}^\mathbf{T}\mathbf{A}\mathbf{e}_\mathbf{J}\right) + C}{\varphi\mathbf{e}_\mathbf{J}^\mathbf{T}\mathbf{A}\mathbf{e}_\mathbf{J} + C} \right) \\
& - \frac{1}{2}\log\left(\frac{\varphi\left(\mathbf{e}_\mathbf{T}^\mathbf{T}\mathbf{B}\mathbf{e}_\mathbf{T} + \mathbf{e}_\mathbf{J}^\mathbf{T}\mathbf{B}\mathbf{e}_\mathbf{J}\right)}{e^{2\eta}\mathbf{e}_\mathbf{J}^\mathbf{T}\mathbf{B}\mathbf{e}_\mathbf{J}} \right), 0 \Bigg\}
\end{aligned}
\tag{28}
$$

where $\mathbf{e}_\mathbf{T}$ and $\mathbf{e}_\mathbf{J}$ are the column vectors whose ith and jth entries for $i \in \mathcal{T}$ and $j \in \mathcal{J}$ are all 1's and the others are all 0's, respectively. Finally, the optimal average secrecy rate,

TABLE II. Simulation Parameters

Room configuration	
Length (L) × Width (W)	30×30 m^2
Height from the work plane (H)	2.2 m
Number of light fixtures	36
Number of LEDs per fixture	8
Locations of transmitters	$\{\pm 2.5, \pm 7.5 \pm 12.5\}$
LED electrical and optical characteristics	
Average optical power per LED	1 W
Optical power / current η	5
Nominal half-intensity angle $\Phi_{1/2}$	60°
Modulation index α	0.5
Optical receiver characteristics	
Photodetector's responsivity	0.54 mA/mW
Lens refractive index κ	1.5
Noise power σ^2	-98.33 dBm
Field of View Ψ_c	90°

which is obtained by mapping the continuum model to the discrete model, can be calculated by numerically evaluating

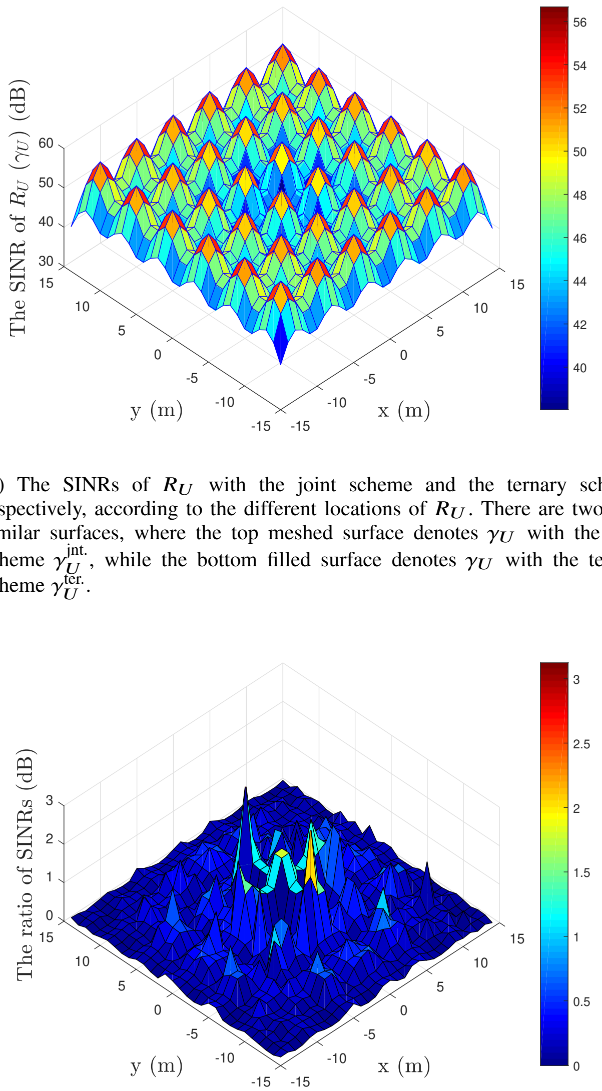
$$\overline{R}^{\star}_{s,\text{disc.}} = \int_{\mathcal{R}_{E_1}}^{\mathcal{R}_{E_2}} \int_0^{2\pi} f_{r_E}(r) R_{s,\text{disc.}}(r,\theta) r \, d\theta \, dr$$
$$= \int_{\mathcal{R}_{E_1}}^{\mathcal{R}_{E_2}} \int_0^{2\pi} \frac{2r^2}{\mathcal{R}_{E_2}^2 - \mathcal{R}_{E_1}^2} R_{s,\text{disc.}}(r,\theta) \, d\theta \, dr. \quad (29)$$

VI. Numerical Results

In this section, we provide numerical results to verify the performances of the proposed joint strategies. The room configuration and simulation parameters are provided in Table II. We use the Cartesian coordinate system to identify positions of transmitters and receivers, where the center of the room is located at the origin.

A. Signal-to-Interference-plus-Noise Ratio

Fig. 7 shows the comparison of the SINR of R_U for the joint scheme and the ternary scheme according to the location of R_U. The optimal beamforming weight and jamming intensity vectors for the given location of R_U are obtained by solving the optimization problems (13) and (17), respectively, and the SINRs of R_U are plotted according to the locations of R_U in Fig. 7(a). In the figure, there are two very similar surfaces, where the top meshed surface corresponds to the joint scheme denoted by $\gamma_U^{\text{jnt.}}$, while the bottom filled surface relates to the ternary scheme denoted by $\gamma_U^{\text{ter.}}$. As seen in the figure, the performances of the joint scheme and the ternary scheme with respect to γ_U are so similar that it is difficult to observe their difference. To clarify the gap between the two surfaces, the ratio of SINRs is plotted on a dB scale, i.e., $10 \times \log_{10}(\gamma_U^{\text{jnt.}}/\gamma_U^{\text{ter.}})$, according to location of R_U in Fig. 7(b). The figure shows that the two proposed schemes yield a similar performance in most of the area, while the joint scheme shows slightly better performance at the center of the room. Considering that the complexity in solving the optimization problem for the joint scheme (13) is much higher than that of the ternary scheme (17), the small performance gap indicates that the ternary scheme may be preferred in practice.

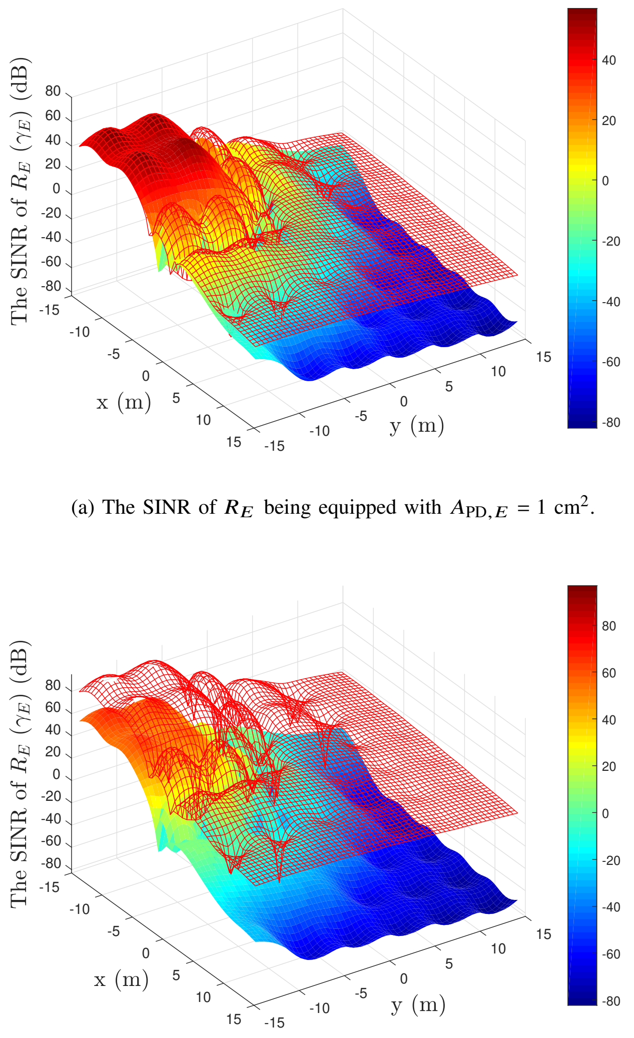


(a) The SINRs of R_U with the joint scheme and the ternary scheme, respectively, according to the different locations of R_U. There are two very similar surfaces, where the top meshed surface denotes γ_U with the joint scheme $\gamma_U^{\text{jnt.}}$, while the bottom filled surface denotes γ_U with the ternary scheme $\gamma_U^{\text{ter.}}$.

(b) The ratio of SINRs generalized by the ternary scheme, i.e., $10 \times \log_{10}(\gamma_U^{\text{jnt.}}/\gamma_U^{\text{ter.}})$

Fig. 7. The comparison of the SINRs of R_U between the joint strategy and the ternary strategy. $\overline{\rho}_E = 0.3$ is used for the optimizations.

Fig. 8 shows the SINRs of R_E with the joint scheme and the beamforming, respectively, as a function of the R_E locations. The beamforming scheme [20] is given as a benchmark in which the beamforming vector (without jamming) can be calculated without the knowledge on the locations or CSI of R_E like the proposed joint scheme. In the figure, there are two surfaces, where the top meshed surface is for the beamforming-only method, while the bottom filled surface is for the joint scheme. Here, R_U is located at $(-10.5, -10.5)$. For a fair comparison, $\gamma_U = 46$ dB is set for both the joint scheme and the beamforming-only approach. In (a), it is shown that, for both the schemes, the SINR of R_E is very high when R_E is close to the R_U location, but it decreases very quickly as R_E moves away from R_U because the channel gain decays like $l^{(m+3)}$. However, at the faraway locations from R_U, γ_E with the



(a) The SINR of R_E being equipped with $A_{\text{PD},E} = 1$ cm^2.

(b) The SINR of R_E being equipped with $A_{\text{PD},E} = 100$ cm^2.

Fig. 8. The comparison for the SINRs of R_E between the joint strategy and the beamforming according to the different locations of R_E. The top meshed surface is for the beamforming-only method, while the bottom filled surface is for the joint scheme. In both figures, R_U is located at $(-10.5, -10.5)$ and equipped with $A_{\text{PD},U} = 1$ cm^2, while R_E has a larger PD $A_{\text{PD},E} = 100$ cm^2 in (b). For a fair comparison, $\gamma_U = 46$ dB is set for both of the joint scheme and the beamforming.

joint scheme is much lower than that with the beamforming-only technique due to the presence of the jammers there.

On the other hand, the fact that γ_E at the distant location is much lower than γ_U with both schemes might evoke a thought that the beamforming scheme itself is enough to ensure a secure connection unless R_E is located near to R_U. However, in reality, the possible eavesdropping scenario in VLC systems can include the eavesdropper with dominant receiver front-end specifications much better than those of the legitimate user, such as a larger physical PD area, a higher PD responsivity, a higher refractive index, etc. Moreover, in our earlier work [21], it was shown that the collusion of multiple eavesdroppers could achieve a high diversity gain to improve the SNR of the eavesdroppers, which results in the increase of the secrecy outage probability (SOP). Thus, due to these facts, lowering the eavesdropper's SINR as much as possible would be essential for securing the transmission even when the SINR of a legitimate user is higher than that of an eavesdropper with the same specification of receiver device.

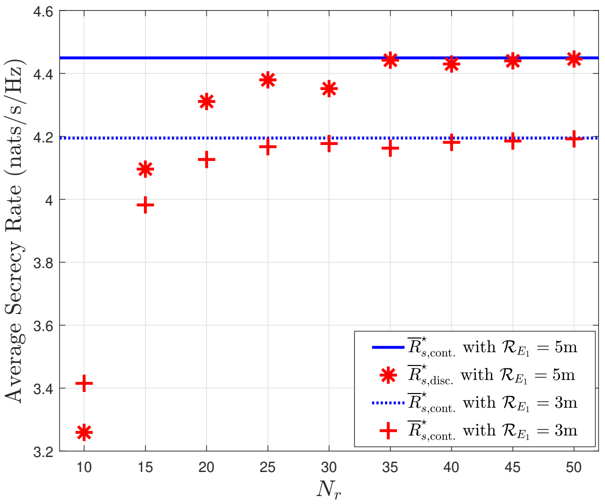


Fig. 9. The optimized average secrecy rates of the continuum model and its corresponding discrete model for the different number of transmitters $N = N_r \times N_r$. For the discrete model, R_U is assumed to be located at $(0,0)$ in 30×30 m^2 room and R_E is assumed to be uniformly and randomly located in the annulus plane centered at $(0,0)$ with inner radius $\mathcal{R}_{E_1}$ and outer radius $\mathcal{R}_{E_2} = 15$ m. $\sigma_T = 0.62$ is used. $\overline{R}^\star_{s,\text{cont.}}$ and $\overline{R}^\star_{s,\text{disc.}}$ correspond to (23) and (29), respectively.

From this perspective, Fig. 8(b) shows how effectively the proposed joint scheme reduces the SINR of R_E being equipped with a larger PD[5]. In (b), the physical area of the PD of R_E ($A_{\text{PD},E} = 100$ cm^2) is set much larger than that of R_U ($A_{\text{PD},E} = 1$ cm^2). For the beamforming scheme, it is shown that R_E is able to significantly improve its SINR up to 40 dB over the entire room by increasing the PD size, compared to Fig. 8(a). However, for the joint scheme, it is shown that γ_E slightly increases near the location of R_U, while it remains almost unchanged in the distant area. This is because R_E receives more of the jamming signals as well as the information signals through the larger PD; it cannot increase its SINR just by increasing the PD size. In addition, the probability of the secrecy connectivity [27], which can be defined as $P_{sc} = \mathbb{P}(\gamma_U > \gamma_E)$, decreases from 0.94 to 0.75 with the beamforming scheme, while it slightly changes from 0.93 to 0.90 with the joint scheme.

B. Secrecy Rate with the Continuum Model

Fig. 9 shows the optimized average secrecy rate of the continuum model and its corresponding discrete model according to different numbers of transmitters in order to demonstrate the validity of the continuum model. As the number of transmitters $N = N_r \times N_r$ increases, it is shown that the average secrecy

[5] Considering the channel model in (2), other better specifications of the eavesdropper can be considered in the same way.

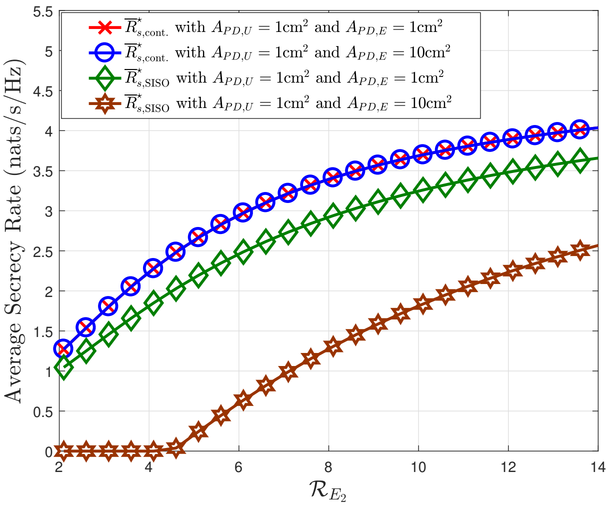


Fig. 10. The optimized average secrecy rate $\overline{R}^{\star}_{s}$ for the different sizes of PD. R_E is assumed to be uniformly and randomly located in the gray annulus plane with inner radius $\mathcal{R}_{E_1} = 2$ m and outer radius $\mathcal{R}_{E_2}$. $\sigma_T = 0.62$ is used.

rate of the discrete model converges to that of the continuum model. More specifically, when the 10×10 discrete LEDs are present in a 30×30 m^2 area, the gap between $\overline{R}^{\star}_{s,\text{cont.}}$ and $\overline{R}^{\star}_{s,\text{disc.}}$ is 0.78 nats/s/Hz for $\mathcal{R}_{E_1} = 3$m. However, when the number of transmitters is larger than 20×20, the gap rapidly decreases to less than 0.07 nats/s/Hz. This result verifies that the continuum model well approximates the real VLC systems that have an adequately large number of LEDs.

Fig. 10 shows the performance of the ternary scheme regarding the average secrecy rate. For comparison, the SISO transmission [9] is given as a benchmark, whose secrecy rate expression with the continuum model and with assuming that the input signal follows the truncated Gaussian distribution is given by

$$R_{s,\text{SISO}} = \frac{1}{2}\log\left(\frac{\sigma_T^2\zeta_U^2 P_D^2(0)e^{2\eta} + \sigma^2}{\sigma_T^2\zeta_E^2 P_D^2(r_E)\varphi + \sigma^2}\right). \tag{30}$$

See Appendix A-B for the proof. Then, we numerically solve the optimization problem maximizing the average secrecy rate for the SISO transmission, i.e.,

$$\overline{R}^{\star}_{s,\text{SISO}} = \max_{\mathcal{R}_T} \overline{R}_{s,\text{SISO}} \tag{31}$$

where

$$\overline{R}_{s,\text{SISO}} = \int_{\mathcal{R}_{E_1}}^{\mathcal{R}_{E_2}} \frac{2r}{\mathcal{R}_{E_2}^2 - \mathcal{R}_{E_1}^2} R_{s,\text{SISO}}(r)\,\mathrm{d}r. \tag{32}$$

In the figure, it is shown that the ternary scheme slightly outperforms the SISO transmission over the entire region of $\mathcal{R}_{E_2}$ when the physical areas of PD for R_U and R_E are identically 1 cm^2. More specifically, when $\mathcal{R}_{E_2}$ is small, in which case R_E is likely to be located nearer to R_U, the gap between $\overline{R}^{\star}_{s,\text{cont.}}$ and $\overline{R}^{\star}_{s,\text{SISO}}$ is small. This is because the jamming signals emitted from the near jammers would not be beneficial since the jamming signals would hamper even the information transmission from the LEDs to R_U. On the other hand, when $\mathcal{R}_{E_2}$ is large; thus R_E is likely to be located at distant positions from R_U, R_E cannot wiretap the information signal even without the jamming signals present because the channel gain in VLC systems decays very quickly according to the distance from the LEDs to the receiver. Therefore, the secrecy rate with the SISO transmission is similar to, but slightly less than, the ternary scheme. However, when the PD size of R_E increases to 10 cm^2, it is shown that the gap between $\overline{R}^{\star}_{s,\text{cont.}}$ and $\overline{R}^{\star}_{s,\text{SISO}}$ becomes significant because R_E being equipped with a large PD is able to more effectively eavesdrop the information signal even at distant locations under the SISO transmission. However, under the ternary scheme, R_E cannot increase its eavesdropping ability by increasing its PD size; thus the average secrecy rate remains unchanged.

Figs. 11(a), (b) and (c) show the secrecy rate performance as a function of R_E locations for the three proposed schemes, i.e., the joint scheme, the ternary scheme and the continuum model (but transformed to the discrete model by utilizing the method described in Section V-D), respectively. In (a) and (b), as we mentioned in Section III-B, the two schemes perform in the way that the near LEDs act as the information transmitters, while all of the other distant LEDs act as the jammers. In (c), the continuum model performs in a similar way, except that the locations of jammers are slightly nearer to R_U than (a) and (b), reducing the low secrecy rate region (e.g., less than 3 nats/s/Hz). Although the beamforming and jamming vectors for the first two schemes are obtained from the suboptimal optimization problems maximizing the SINR of R_U, it is shown that these schemes also perform well in terms of maximizing the secrecy rate. Under the assumption that R_E is randomly located in a circle with radius 15 m centered at R_U, the average secrecy rates for the joint scheme and the ternary scheme are 3.85 nats/s/Hz and 3.83 nats/s/Hz, respectively, while the continuum model yields 3.91 nats/s/Hz.

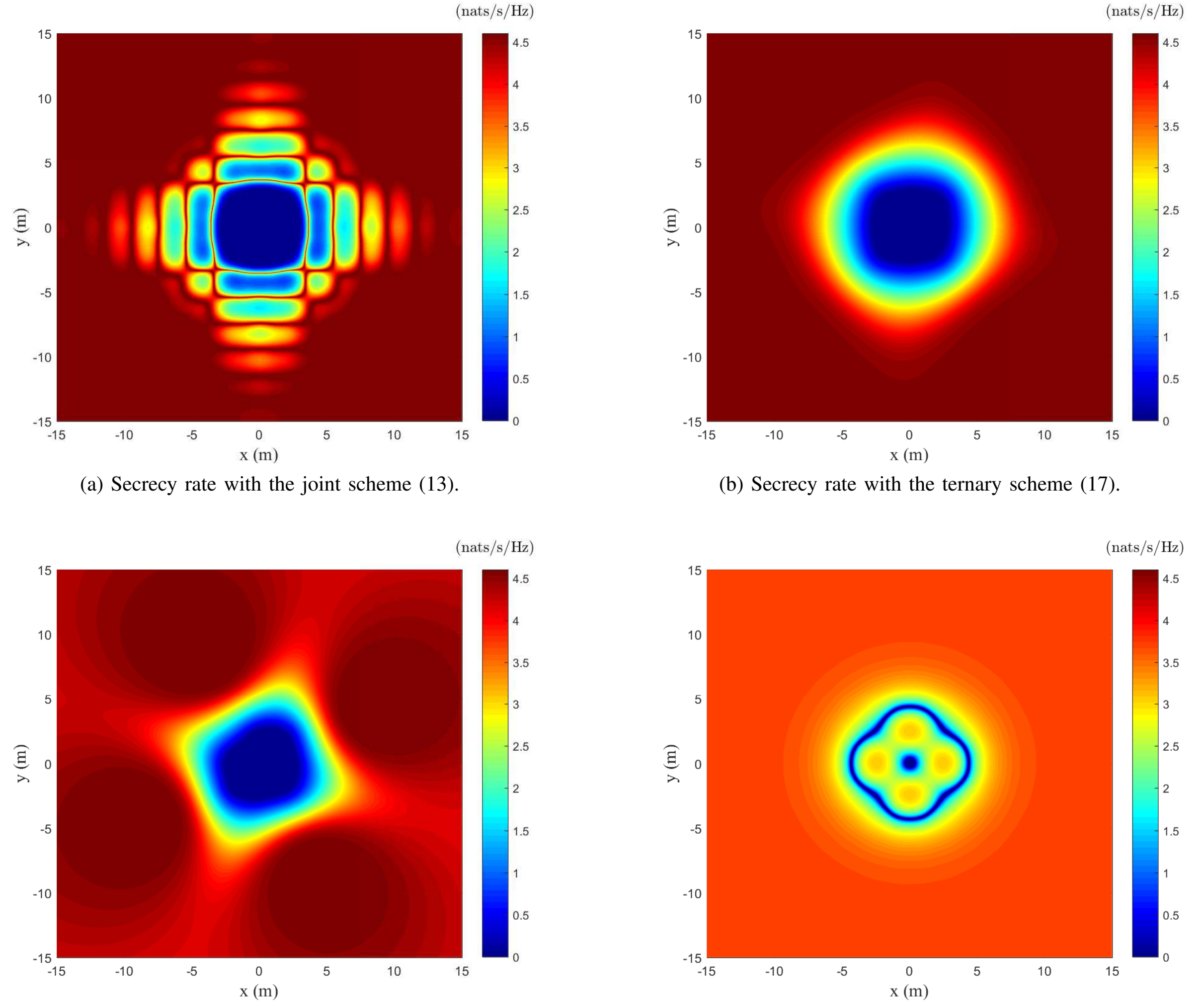
In addition, to compare the proposed joint scheme with the existing jamming scheme that does not require knowledge of the location of an eavesdropper, the secrecy rate under the artificial noise scheme [10] is given in Fig. 11(d). The beamforming and jamming vectors for the artificial noise can be obtained as

$$\mathbf{w}_{\text{AN}} = k\rho\alpha I_{DC}\hat{\mathbf{h}}_U, \quad \mathbf{v}_{\text{AN}} = k\alpha I_{DC}\frac{1-\rho}{N-1}\sum_{i=1}^{N-1}\hat{\varphi}_{\text{B}_i}$$

respectively, where $\hat{\mathbf{h}}_U = \mathbf{h}_U/||\mathbf{h}_U||_1$, and $\hat{\varphi}_{\text{B}_i} \in \mathbb{R}^N$ for $i \in \{1, 2, ..., N-1\}$ constitute a basis for the nullspace of $\mathbf{h}_U^T$ and are normalized such that $||\hat{\varphi}_{\text{B}_i}||_1 = 1, \forall i \in \{1, 2, ..., N-1\}$. k is a constant such that the peak constraint

$$k\left(\rho|\hat{\mathbf{h}}_B| + \frac{1-\rho}{N-1}\sum_{i=1}^{N-1}|\hat{\varphi}_{B_i}|\right) \preceq \mathbb{1}$$

is satisfied. Also, ρ is the parameter that determines the optical power fraction devoted to a data signal, while $1-\rho$ is for jamming signals. In Fig. 11(d), it is shown that the secrecy rate with the artificial noise is less than the continuum model in Fig. 11(c) at the outer area of the room, while higher near



(a) Secrecy rate with the joint scheme (13).

(b) Secrecy rate with the ternary scheme (17).

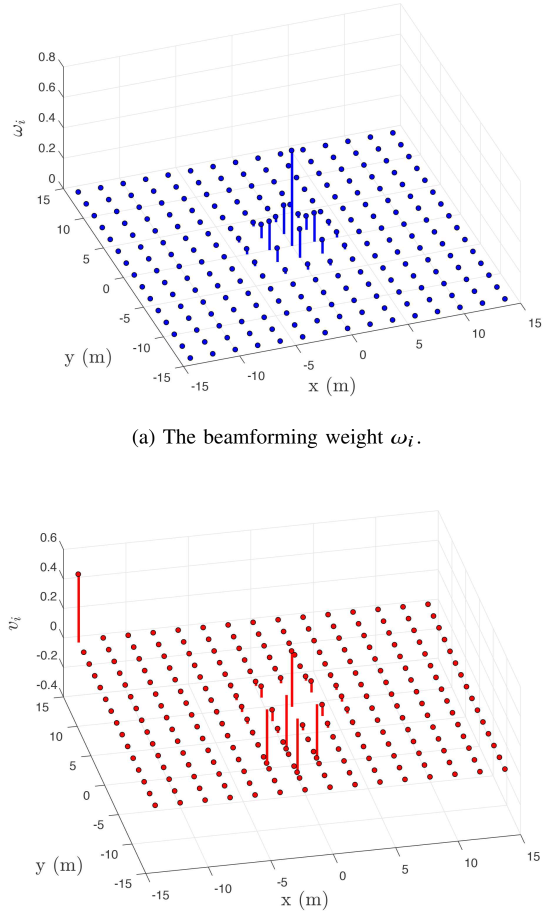
(c) Secrecy rate with the continuum model transformed to the discrete model using the procedure in Section V-D.

(d) Secrecy rate with the artificial noise in [10]. $\rho = 0.5$ is used.

Fig. 11. The comparison of secrecy rates under the different proposed schemes, the joint scheme, the ternary scheme, the continuum model, and the artificial noise transmission according to the location of R_E. R_U is located at $(0, 0)$ and 15×15 LEDs are uniformly distributed on a square lattice in 30×30 m^2 room. For the continuum model, $\mathcal{R}_{E_1} = 0$ m and $\mathcal{R}_{E_1} = 15$ m are used.

around R_U. This result shows that transmitting the artificial noise (jamming) signals towards the nullspace of R_U yields a higher secrecy performance at the small area near to R_U by not causing the interference at R_U site, but it does not perform in a way that maximizes the secrecy performance. Under the assumption that R_E is randomly located in the room, the average secrecy rate for the artificial noise is 3.50 nats/s/Hz, while the continuum model yields 4.01 nats/s/Hz. The reason can be more understandable by observing the beamforming and jamming vectors $\mathbf{w}_{\text{AN}}, \mathbf{v}_{\text{AN}}$ in Fig. 12. It is noted that the beamforming weight of the nearest LED to R_U is $\omega_{\text{nrst.}} = 0.62$, not 1, because the fraction $1 - \rho$, i.e., $\nu_{\text{nrst.}} = 0.38$, is allocated to suppress the interference at R_U site. Since the channel gain largely depends on the distance between transmitter and receiver, the power allocation of the nearest LED for the jamming signals would significantly reduce the received optical power of the information signal at R_U site. In general, the decrease of the information reception at R_U would result in the degradation of the average secrecy performance, instead, it would be better to allow the small interference at R_U site and allocate the whole power of the nearest LED to transmit the information signal as our proposed schemes behave. Moreover, although the jamming signal precoded by $\mathbf{v}_{\text{AN}}$ does not cause interference at R_U site, most all the jamming intensities at faraway locations from R_U are almost zero. In this case, the artificial noise scheme cannot take advantage of the jamming signals at the large outer area. Considering a practical scenario that the eavesdropper equipped with a powerful receiver would like to be located not too near to the intended user to escape the vigilance of the legitimate user, the proposed joint scheme can be more preferred.

Fig. 13 shows the SOP for the three proposed schemes, the artificial noise transmission [10], and the SISO transmission [9] with the same room configuration of Fig. 11, where the SOPs of the last two schemes are given as benchmarks. R_E is assumed to be randomly located in a circle with radius 15 m centered at R_U. The SOP is defined as the probability that the secrecy capacity C_s is less than a threshold secrecy



(a) The beamforming weight ω_i.

(b) The jamming intensity ν_i.

Fig. 12. The beamforming and jamming vectors with the artificial noise [10]. R_U is located at $(0, 0, 0)$. The 15×15 LED transmitters are uniformly distributed on a square lattice in the 30×30 m^2 room. $H = 2.2$ m, $\phi_{1/2} = 60°$ and $\rho = 0.5$ are used.

capacity C_{th}, i.e., $P_{\text{SO}} = \mathbb{P}(C_s < C_{th})$ [43]. However, since the closed-form of the secrecy capacity with the input amplitude constraint is not readily available, we employ the secrecy rate in (9) to determine the secrecy outage; thus the SOP can be defined as $P_{\text{SO}} = \mathbb{P}(R_s < R_{th})$, where R_{th} denotes the threshold secrecy rate. Fig. 13 shows that all the proposed joint schemes and the artificial noise scheme outperform the SISO transmission, i.e., they have much lower SOPs over the entire region. Also, the SOPs of the joint and ternary schemes are similar to each other, while the continuum model has slightly lower SOP than the two schemes at the region up to 4.1 nats/s/Hz. In contrast, the artificial noise yields the lowest SOP among the four schemes at the region up to 3 nats/s/Hz, while it radically increases after 3.6 nats/s/Hz. This result shows that the proposed three schemes have better secrecy performance, i.e., lower SOP than the artificial noise transmission at the region of high R_{th}. Note that an eavesdropper generally prefers to stay at the outer area of the room, where the secrecy rate appears high, escaping the vigilance of the legitimate user.

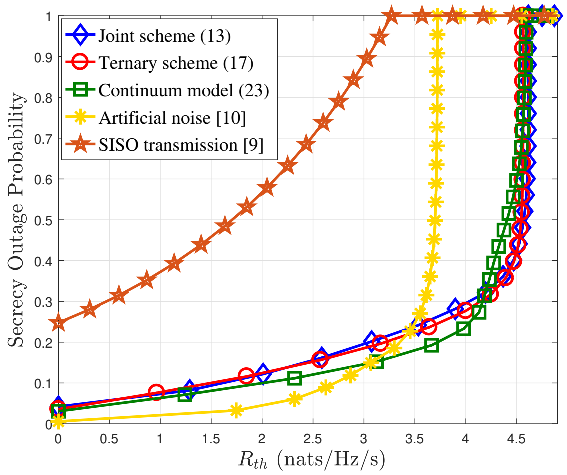


Fig. 13. The secrecy outage probability under the different proposed schemes, such as the joint scheme, the ternary scheme, the continuum model, and the artificial noise transmission. R_U is located at $(0, 0)$ and 15×15 LEDs are uniformly distributed on a square lattice in 30×30 m^2 room. $A_{\text{PD},E} = 10$ cm^2 is used.

VII. Conclusion

In this paper, we studied simultaneous beamforming and jamming strategies when an eavesdropper is randomly located; thus its location or the CSI is not available at the transmitter. First, we formulated the optimization problem of maximizing the SINR of the intended user while constraining the SINR of the eavesdropper, and we then solved it by utilizing the CCP heuristic method. Then, we proposed a simpler ternary scheme that is much less complicated and obtained its solution by using TS. The numerical results verified that the ternary scheme provides an excellent practical solution to enhancing the secrecy performance without incurring a high computation complexity. Moreover, by utilizing a continuous LED model, the maximization of the average secrecy rate under the ternary scheme was investigated. Our results render useful insight and analytic tools that can be used to increase security in VLC systems, and they provide a solid basis for further study.

Appendix A
Derivation of the Lower Bound on Secrecy Capacity

A. Secrecy Rate with the Joint Technique of Beamforming and Jamming

A lower bound on the secrecy rate of (6) can be obtained as follows

$$\begin{aligned} C_s &= \max_{p_X, p_J} \left(\mathbb{I}(X; Y_U) - \mathbb{I}(X; Y_E) \right) \\ &\overset{(a)}{\geq} \mathbb{I}(X; Y_U) - \mathbb{I}(X; Y_E) \\ &\overset{(b)}{\geq} \mathbb{I}(X; Y_U) - \mathbb{I}(X; V_E) \\ &= \mathbb{h}(Y_U) - \mathbb{h}(Y_U|X) - \mathbb{h}(V_E) + \mathbb{h}(V_E|X) \end{aligned} \tag{33}$$

where $\mathbb{h}(\cdot)$ denotes differential entropy and $V_E = \alpha I_{DC} \mathbf{h}_{\mathbf{E}}^{\mathbf{T}} \mathbf{w} X + \alpha I_{DC} \mathbf{h}_{\mathbf{E}}^{\mathbf{T}} \mathbf{v} J$. (a) follows from dropping the maximization by choosing a truncated Gaussian distribution on p_X and p_J, and (b) follows from the data-processing inequality, i.e., $Y_E = g(V_E) = V_E + N_E$. Firstly, we lower-bound $\mathbb{h}(Y_U)$ by using the entropy-power inequality as

$$\begin{aligned}\mathbb{h}(Y_U) &\geq \frac{1}{2}\log\left(e^{2\mathbb{h}(\alpha I_{DC}\mathbf{h}_{\mathrm{U}}^{\mathbf{T}}\mathbf{w}X)} + e^{2\mathbb{h}(\alpha I_{DC}\mathbf{h}_{\mathrm{U}}^{\mathbf{T}}\mathbf{v}J)} + e^{2\mathbb{h}(N_U)}\right)\\ &= \frac{1}{2}\log\left(2\pi e\left(\sigma_T^2\alpha^2 I_{DC}^2(\mathbf{w}^{\mathbf{T}}\mathbf{A}\mathbf{w} + \mathbf{v}^{\mathbf{T}}\mathbf{A}\mathbf{v})e^{2\eta} + \sigma^2\right)\right)\end{aligned} \tag{34}$$

where (34) follows from the facts that

$$\mathbb{h}\left(\alpha I_{DC}\mathbf{h}_{\mathbf{U}}^{\mathbf{T}}\mathbf{w}X\right) = \log\left(\left|\alpha I_{DC}\mathbf{h}_{\mathbf{U}}^{\mathbf{T}}\mathbf{w}\right|\right) + \frac{1}{2}\log\left(2\pi e\sigma_T^2\right) + \eta, \tag{35a}$$

$$\mathbb{h}\left(\alpha I_{DC}\mathbf{h}_{\mathbf{U}}^{\mathbf{T}}\mathbf{v}J\right) = \log\left(\left|\alpha I_{DC}\mathbf{h}_{\mathbf{U}}^{\mathbf{T}}\mathbf{v}\right|\right) + \frac{1}{2}\log\left(2\pi e\sigma_T^2\right) + \eta, \tag{35b}$$

$$\mathbb{h}\left(N_U\right) = \frac{1}{2}\log 2\pi e\sigma^2. \tag{35c}$$

Then, we upper-bound $\mathbb{h}(Y_U|X)$ and $\mathbb{h}(V_E)$ as

$$\begin{aligned}\mathbb{h}\left(Y_U|X\right) &= \mathbb{h}\left(Y_U - \alpha I_{DC}\mathbf{h}_{\mathbf{U}}^{\mathbf{T}}\mathbf{w}X|X\right) = \mathbb{h}\left(\alpha I_{DC}\mathbf{h}_{\mathbf{U}}^{\mathbf{T}}\mathbf{v}J + N_U\right)\\ &\leq \frac{1}{2}\log 2\pi e\left(\sigma_T^2\alpha^2 I_{DC}^2\mathbf{v}^{\mathbf{T}}\mathbf{A}\mathbf{v}\varphi + \sigma^2\right) \qquad (36)\\ \mathbb{h}\left(V_E\right) &= \mathbb{h}\left(\alpha I_{DC}\mathbf{h}_{\mathbf{E}}^{\mathbf{T}}\mathbf{w}X + \alpha I_{DC}\mathbf{h}_{\mathbf{E}}^{\mathbf{T}}\mathbf{v}J\right)\\ &\leq \frac{1}{2}\log 2\pi e\left(\sigma_T^2\alpha^2 I_{DC}^2(\mathbf{w}^{\mathbf{T}}\mathbf{B}\mathbf{w} + \mathbf{v}^{\mathbf{T}}\mathbf{B}\mathbf{v})\varphi\right) \qquad (37)\end{aligned}$$

by using the differential entropy of Gaussian random variables with variances $\mathbb{V}\mathrm{ar}\{\alpha I_{DC}\mathbf{h}_{\mathbf{U}}^{\mathbf{T}}\mathbf{v}J + N_U\}$ and $\mathbb{V}\mathrm{ar}\{\alpha I_{DC}\mathbf{h}_{\mathbf{E}}^{\mathbf{T}}\mathbf{w}X + \alpha I_{DC}\mathbf{h}_{\mathbf{E}}^{\mathbf{T}}\mathbf{v}J\}$, respectively. Lastly, we have

$$\begin{aligned}\mathbb{h}\left(V_E|X\right) &= \mathbb{h}\left(V_E - \alpha I_{DC}\mathbf{h}_{\mathbf{E}}^{\mathbf{T}}\mathbf{w}X|X\right) = \mathbb{h}\left(\alpha I_{DC}\mathbf{h}_{\mathbf{E}}^{\mathbf{T}}\mathbf{v}J\right)\\ &= \frac{1}{2}\log\left(2\pi e\alpha^2 I_{DC}^2\mathbf{v}^{\mathbf{T}}\mathbf{B}\mathbf{v}\sigma_T^2\right) + \eta.\end{aligned} \tag{38}$$

Plugging (34), (36), (37) and (38) into (33) yields the secrecy rate for the joint technique in (9).

B. Secrecy Rate with the SISO channel

With the SISO transmission under the continuum model, the received signals for R_U and R_E are given by

$$y_U(t) = \zeta_U P_D(0)x + n_U, \tag{39a}$$

$$y_E(t) = \zeta_E P_D(r_E)x + n_E. \tag{39b}$$

Then, a lower bound on the secrecy rate of (39) can be obtained as follows

$$\begin{aligned}C_s &= \max_{p_X}\left(\mathbb{I}(X;Y_U) - \mathbb{I}(X;Y_E)\right)\\ &\overset{(a)}{\geq} \mathbb{I}(X;Y_U) - \mathbb{I}(X;Y_E)\\ &= \mathbb{h}(Y_U) - \mathbb{h}(Y_U|X) - \mathbb{h}(Y_E) + \mathbb{h}(Y_E|X)\\ &= \mathbb{h}(Y_U) - \mathbb{h}(N_U) - \mathbb{h}(Y_E) + \mathbb{h}(N_E) = \mathbb{h}(Y_U) - \mathbb{h}(Y_E)\\ &\overset{(b)}{\geq} \frac{1}{2}\log\left(e^{2\mathbb{h}(\zeta_U P_D(0)X)} + e^{2\mathbb{h}(N_U)}\right) - \frac{1}{2}\log 2\pi e\mathbb{V}\mathrm{ar}\{Y_E\}\\ &= \frac{1}{2}\log\left(2\pi e(\sigma_T^2\zeta_U^2 P_D^2(0)e^{2\eta} + \sigma^2)\right)\\ &\quad - \frac{1}{2}\log\left(2\pi e(\sigma_T^2\zeta_E^2 P_D^2(r_E)\varphi + \sigma^2)\right)\\ &= \frac{1}{2}\log\left(\frac{\sigma_T^2\zeta_U^2 P_D^2(0)e^{2\eta} + \sigma^2}{\sigma_T^2\zeta_E^2 P_D^2(r_E)\varphi + \sigma^2}\right)\end{aligned} \tag{40}$$

where, similarly, (a) follows from dropping the maximization by choosing a truncated Gaussian distribution on p_X, and (b) follows by lower-bounding $\mathbb{h}(Y_U)$ using the entropy-power inequality and upper-bounding $\mathbb{h}(Y_E)$ using the differential entropy of a Gaussian random variable with variance $\mathbb{V}\mathrm{ar}\{\zeta_E P_D(r_E)x + n_E\}$.

References

[1] M. Ayyash, H. Elgala, A. Khreishah, V. Jungnickel, T. Little, S. Shao, M. Rahaim, D. Schulz, J. Hilt, and R. Freund, "Coexistence of WiFi and LiFi toward 5G: Concepts, opportunities, and challenges," *IEEE Commun. Mag.*, vol. 54, no. 2, pp. 64–71, 2016.

[2] D. Karunatilaka, F. Zafar, V. Kalavally, and R. Parthiban, "LED based indoor visible light communications: State of the art," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1649–1678, 2015.

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

[4] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[5] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, Jan. 1975.

[6] D. W. K. Ng, E. S. Lo, and R. Schober, "Robust beamforming for secure communication in systems with wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 13, no. 8, pp. 4599–4615, Aug. 2014.

[7] G. Chen, J. P. Coon, and M. D. Renzo, "Secrecy outage analysis for downlink transmissions in the presence of randomly located eavesdroppers," *IEEE Trans. Inf. Forens. Security*, vol. 12, no. 5, pp. 1195–1206, May 2017.

[8] J. Zhu, R. Schober, and V. K. Bhargava, "Linear precoding of data and artificial noise in secure massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, pp. 2245–2261, Mar. 2016.

[9] 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.

[10] ——, "Physical-layer security for indoor visible light communications," in *IEEE ICC in Sydney, Australia*, Jun. 2014, pp. 3342–3347.

[11] ——, "Securing visible light communications via friendly jamming," in *IEEE Globecom Workshops in Austin, USA*, Dec. 2014, pp. 524–529.

[12] ——, "Pattern synthesis of massive LED arrays for secure visible light communication links," in *IEEE ICCW in London, U.K.*, Jun. 2015, pp. 1350–1355.

[13] ——, "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.

[14] H. Zaid, Z. Rezki, A. Chaaban, and M. S. Alouini, "Improved achievable secrecy rate of visible light communication with cooperative jamming," in *IEEE GlobalSIP in Orlando, U.S.A.*, Dec. 2015, pp. 1165–1169.

[15] M. A. Arfaoui, Z. Rezki, A. Ghrayeb, and M. S. Alouini, "On the secrecy capacity of MISO visible light communication channels," in *IEEE Globecom in Washington D.C., USA*, Dec. 2016, pp. 1–7.

[16] T. V. Pham, H. Le-Minh, and A. T. Pham, "Multi-user visible light communication broadcast channels with zero-forcing precoding," *IEEE Trans. Commun.*, vol. 65, no. 6, pp. 2509–2521, Jun. 2017.

[17] T. V. Pham, T. Hayashi, and A. T. Pham, "Artificial-noise-aided precoding design for multi-user visible light communication channels," *IEEE Access*, pp. 1–1, 2018.

[18] M. A. Arfaoui, A. Ghrayeb, and C. M. Assi, "Secrecy performance of multi-user MISO VLC broadcast channels with confidential messages," *IEEE Trans. Wireless Commun.*, vol. 17, no. 11, pp. 7789–7800, Nov. 2018.

[19] S. Cho, G. Chen, and J. P. Coon, "Secrecy analysis in visible light communication systems with randomly located eavesdroppers," in *IEEE ICC Workshops in Paris, France*, May 2017, pp. 475–480.

[20] ——, "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] ——, "Physical layer security in visible light communication systems with randomly located colluding eavesdroppers," *IEEE Wireless Commun. Lett.*, vol. 7, no. 5, pp. 768–771, Oct. 2018.

[22] J. M. Hamamreh, H. M. Furqan, and H. Arslan, “Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey,” *IEEE Commun. Surveys Tuts.*, pp. 1–1, 2018.

[23] M. Obeed, A. M. Salhab, M. Alouini, and S. A. Zummo, “On optimizing VLC networks for downlink multi-user transmission: A survey,” *CoRR*, vol. abs/1808.05089, 2018. [Online]. Available: http://arxiv.org/abs/1808.05089

[24] I. Marin-Garcia, V. Guerra, and R. Perez-Jimenez, “Study and Validation of Eavesdropping Scenarios over a Visible Light Communication Channel,” *Sensors*, vol. 17, no. 12, p. 2687, 2017.

[25] H. Shen, Y. Deng, W. Xu, and C. Zhao, “Secrecy-oriented transmitter optimization for visible light communication systems,” *IEEE Photon. J*, vol. 8, no. 5, 2016.

[26] G. Geraci, S. Singh, J. G. Andrews, J. Yuan, and I. B. Collings, “Secrecy rates in broadcast channels with confidential messages and external eavesdroppers,” *IEEE Trans. Wireless Commun.*, vol. 13, no. 5, pp. 2931–2943, May 2014.

[27] P. C. Pinto, J. Barros, and M. Z. Win, “Secure communication in stochastic wireless networksPart I: Connectivity,” *IEEE Trans. Inf. Forens. Security*, vol. 7, no. 1, pp. 125–138, Feb 2012.

[28] T. Lipp and S. Boyd, “Variations and extension of the convex–concave procedure,” *Optimization and Engineering*, vol. 17, no. 2, pp. 263–287, Jun. 2016.

[29] A. Lapidoth, S. M. Moser, and M. A. Wigger, “On the capacity of free-space optical intensity channels,” *IEEE Trans. Inf. Theory*, vol. 55, no. 10, pp. 4449–4461, Oct. 2009.

[30] J. Wang, C. Liu, J. Wanga, Y. Wu, M. Lin, and J. Cheng, “Physical-layer security for indoor visible light communications: Secrecy capacity analysis,” *IEEE Trans. Commun.*, pp. 1–1, 2018.

[31] H. Wang, X. Zhou, and M. C. Reed, “Physical layer security in cellular networks: A stochastic geometry approach,” *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2776–2787, 2013.

[32] 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, 2017.

[33] 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.

[34] O. Ozel, E. Ekrem, and S. Ulukus, “Gaussian wiretap channel with an amplitude constraint,” in *IEEE Inf. Theory Workshop in Lausanne, Switzerland*, Sep. 2012, pp. 5553–5563.

[35] Z. Rezki and M. Alouini, “Secret-key agreement with public discussion over multi-antenna transmitters with amplitude constraints,” in *IEEE ISIT*, Jun. 2017, pp. 1534–1538.

[36] I. Krikidis, J. S. Thompson, and S. Mclaughlin, “Relay selection for secure cooperative networks with jamming,” *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003–5011, Oct. 2009.

[37] H. Hui, A. L. Swindlehurst, G. Li, and J. Liang, “Secure relay and jammer selection for physical layer security,” *IEEE Signal Process. Lett.*, vol. 22, no. 8, pp. 1147–1151, Aug. 2015.

[38] A. Charnes and W. W. Cooper, “Programming with linear fractional functionals,” *Naval Research Logistics Quarterly*, vol. 9, no. 3-4, pp. 181–186, 1962.

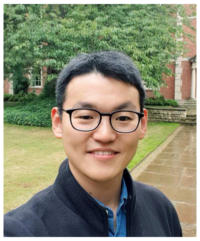
[39] P. T. Boggs and J. W. Tolle, “Sequential quadratic programming,” *Acta Numerica*, vol. 4, p. 151, 1995.

[40] M. R. Garey and D. S. Johnson, *Computers and Intractability; A Guide to the Theory of NP-Completeness*. New York, NY, USA: W. H. Freeman & Co., 1990.

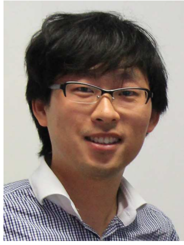
[41] F. Glover and M. Laguna, *Tabu Search*. Norwell, MA, USA: Kluwer Academic Publishers, 1997.

[42] *Lighting of Indoor Work Places*, European Stand. EN 12464-1, 2003.

[43] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, “Wireless information-theoretic security,” *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.



Sunghwan Cho (S’17) received the B.S. degree (summa cum laude) in electrical engineering from the Korea Military Academy, South Korea, in 2007. He earned his M.S. degree in communications from the Georgia Institute of Technology, USA, in 2011. From 2016, he is a DPhil student in the Department of Engineering Science at the University of Oxford, U.K., under the supervision of Professor Justin P. Coon. From 2007, he has worked as an army officer of the Republic of Korea Army, currently holding the rank of a major. His current research interests include physical layer security, stochastic geometry, and visible light communications.



Gaojie Chen (S’09 – M’12 – SM’18) received the B.Eng. and B.Ec. degrees in electrical information engineering and international economics and trade from Northwest University, China, in 2006, and the M.Sc. (Hons.) and Ph.D. degrees in electrical and electronic engineering from Loughborough University, Loughborough, U.K., in 2008 and 2012, respectively. From 2008 to 2009, he was a Software Engineering with DTmobile, Beijing, China, and from 2012 to 2013, he was a Research Associate with the School of Electronic, Electrical and Systems Engineering, Loughborough University. He was a Research Fellow with 5GIC, Faculty of Engineering and Physical Sciences, University of Surrey, U.K., from 2014 to 2015. Then he was a Research Associate with the Department of Engineering Science, University of Oxford, U.K., from 2015 to 2018. He is currently a Lecturer with the Department of Engineering, University of Leicester, U.K. His research interests include information theory, wireless communications, IoT, cognitive radio, secrecy communication and random geometric networks. He received the Exemplary Reviewer Certificate of the IEEE Wireless Communication Letters in 2018. He currently serves as an Editor of the IET Electronics Letters.

Justin P. Coon (S’02 – M’05 – SM’10) received the B.Sc. degree (Hons.) in electrical engineering from the Calhoun Honours College, Clemson University, USA, and the Ph.D. degree in communications from the University of Bristol, U.K., in 2000 and 2005, respectively. In 2004, he joined as a Research Engineer with the Bristol-based Telecommunications Research Laboratory (TRL), Toshiba Research Europe Ltd., where he was involved in research on a broad range of communication technologies and theories, including single- and multi-carrier modulation techniques, estimation and detection, diversity methods, and system performance analysis and networks. He held the research manager position from 2010 to 2013, during which time he led all theoretical and applied research on the physical layer at TRL. He was a Visiting Fellow with the School of Mathematics, University of Bristol, from 2010 to 2012, where he held a reader position with the Department of Electrical and Electronic Engineering from 2012 to 2013. He joined the University of Oxford in 2013, where he is currently an Associate Professor with the Department of Engineering Science and a Tutorial Fellow of Oriel College.

He is the Technical Manager of the EU FP7 project DIWINE. He has authored in excess of 100 papers in leading international journals and conferences, and is a named inventor on over 30 patents. His research interests include communication theory, information theory, and network theory. Dr Coon was a recipient of TRLs Distinguished Research Award for his work on block-spread CDMA, aspects of which have been adopted as mandatory features in the 3GPP LTE Rel-8 standard. He was also a co-recipient of two best paper awards at the ISWCS 2013 and the EuCNC 2014. He received the award for Outstanding Contribution in 2014. He has served as an Editor for the IEEE Transactions on Wireless Communications from 2007 to 2013, the IEEE Transactions on Vehicular Technology from 2013 to 2016. He has been serving as an Editor for the IEEE Wireless Communications Letters since 2016 and the IEEE Communications Letters since 2017.