Physical-Layer Security for Indoor Visible Light Communications

Ayman Mostafa and Lutz Lampe
Department of Electrical and Computer Engineering
The University of British Columbia, Vancouver, BC, V6T 1Z4, Canada
Email: {amostafa,lampe}@ece.ubc.ca

***Abstract*—This paper considers secure transmission over the visible light communication (VLC) channel by the means of physical-layer security techniques. In particular, we consider achievable secrecy rates of the multiple-input, single-output (MISO) wiretap VLC channel. The VLC channel is modeled as a deterministic and real-valued Gaussian channel subject to amplitude constraints. We utilize null-steering and artificial noise strategies to achieve positive secrecy rates when the eavesdropper's channel state information (CSI) is perfectly known and entirely unknown to the transmitter, respectively. In both scenarios, the legitimate receiver's CSI is available to the transmitter. We numerically evaluate achievable secrecy rates under typical VLC scenarios and show that simple precoding techniques can significantly improve the confidentiality of VLC links.**

I. Introduction

Visible light communications (VLC) has emerged as a potential technology for ubiquitous indoor wireless broadband access. It refers to the transmission of information by modulating the intensity of light-emitting diodes (LEDs) at high frequencies making instantaneous changes in light intensity unnoticeable to the human eye. Therefore, VLC technology can exploit the existing lighting infrastructure where legacy tungsten- and florescent-based lamps are being replaced by high-brightness LEDs with longer lifetime, lower power consumption, and higher efficiency.

VLC channels benefit from the unlicensed and virtually-unlimited light spectrum, high signal-to-noise ratio (SNR), immunity to electromagnetic interference, inherent security, and the availability of inexpensive photo-diodes (PDs) as low-cost receivers. Such advantages qualify VLC links to obtain a front seat in next-generation indoor wireless networks. On the other hand, utilizing illumination LEDs and general-purpose PDs for data communication purposes imposes considerable bandwidth and linearity limitations on the underlying VLC channel making high rate transmission a challenging task.

Along with the phenomenal growth of wireless coverage, security and privacy concerns are growing as well. Security measures are typically perceived by end-users as password-protected access, and by network designers as data encryption at layers above the data link and below the application level. However, a simple look at the layered network architecture suggests that the communication network should be secured at all the levels, including the underlying physical layer [1]. Not surprisingly, the interest in physical-layer security has revived during the past years as a part of *multi-layer* security approaches.

The idea of physical-layer security is not new, it dates back to 1970s when Wyner introduced the *degraded* discrete memoryless wiretap channel in his landmark paper [2]. *Secrecy capacity* was defined as the maximum rate of reliable source-destination transmission while the message is entirely hidden from the eavesdropper. In [3], secrecy capacity was obtained for the Gaussian wiretap channel. A single-letter characterization of the secrecy capacity of the general, i.e., *non-degraded*, wiretap channel was obtained by Csiszár and Körner in [4]. The problem of characterizing the secrecy capacity of the Gaussian multiple-input, single-output (MISO) and multiple-input, multiple-output (MIMO) wiretap channel was settled in [5] and [6], respectively. For the Gaussian MISO wiretap channel, it was shown that zero-forcing the eavesdropper's reception via beamforming is optimal at asymptotic high SNR [5]. When the eavesdropper's channel state information (CSI) is unavailable at the transmitter, adding jamming signals, termed as *artificial noise*, to the transmitted data signal was proposed to increase achievable secrecy rates [7], [8].

Due to the line-of-sight propagation and non-penetrating nature of light waves through opaque surfaces, the VLC channel exhibits higher security measures than its radio frequency (RF) counterpart. It is reasonable to consider the VLC link perfectly secure, at the physical layer, in a single-user/private-room scenario. However, in public areas such as classrooms, libraries, hallways, or planes, security of the transmitted signal cannot be guaranteed.

Unlike RF channels, the constrained communication resource in VLC channels is the optical intensity that is directly proportional to the electrical signal amplitude, not to the squared signal as in RF schemes.

This work was supported by the National Sciences and Engineering Research Council of Canada (NSERC).

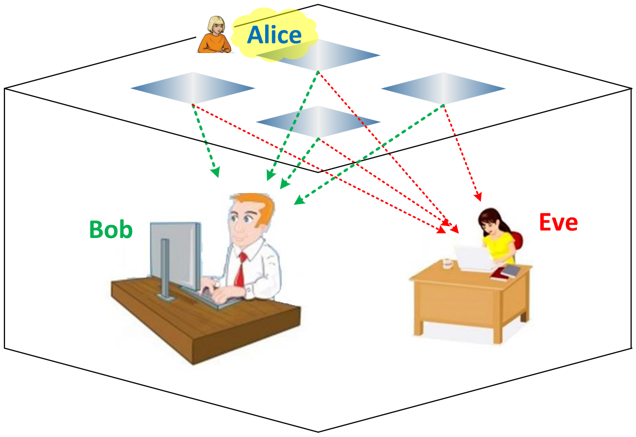

Fig. 1. Physical-layer security for indoor VLC networks.

Therefore, the VLC channel is well-modeled with amplitude, not average power, constraints.

This paper addresses securing indoor VLC links at the physical layer level. We consider achievable secrecy rates of the Gaussian MISO wiretap channel subject to amplitude constraints. Some related works in [9] and [10] considered improving the confidentiality of atmospheric free-space optical (FSO) links via adjusting the magnitude and phase of the transmitted wave along with coherent detection. Unlike RF or FSO related work, this paper considers a VLC scenario with a different topology and different system model.

We first consider the secrecy capacity of the single-input, single-output (SISO) channel, and set it as a benchmark. Then, for the MISO channel, null-steering is utilized to cancel the eavesdropper's reception and fully secure the source-destination rate when the eavesdropper's CSI is available to the transmitter. Without such information, artificial noise is added to the transmitted signal to jam the eavesdropper's reception and improve achievable secrecy rates.

The system model is presented in Sec. II. Secrecy rates are considered in Sec. III. Simulation and numerical results are discussed in Sec. IV. We conclude the paper in Sec. V.

Notation: We refer to the source, destination, and eavesdropper as "Alice", "Bob", and "Eve", respectively. The set of n-dimensional real-valued numbers is denoted by $\mathcal{R}^n$, and the set of n-dimensional non-negative real-valued numbers is denoted by $\mathcal{R}_+^n$. Bold characters denote column vectors, unless otherwise stated. Vector transposition is denoted by the superscript $\{\cdot\}^{\mathrm{T}}$. The all-ones column vector is denoted by $\mathbf{1}$, and its dimension will be clear from the context. The curled inequality symbol $\preceq$ between two vectors denotes componentwise inequality. The vertical bars $|\cdot|$ surrounding a vector denote componentwise absolute value, and $\|\cdot\|_1$ denotes the 1-norm operator. $\{x\}^+$ denotes $\max(x, 0)$. We use SNR to denote the peak, not the average, received signal-to-noise ratio. Probability distribution is denoted by $p(\cdot)$, mutual information by $\mathbb{I}(\cdot;\cdot)$, and expected value by $\mathbb{E}\{\cdot\}$. Subscripts $\{\cdot\}_{\mathrm{B}}$ and $\{\cdot\}_{\mathrm{E}}$ denote Bob's and Eve's relevance, respectively.

II. System Model

We consider the VLC scenario illustrated in Fig. 1. Alice shall exchange confidential messages with Bob in the existence of Eve. In typical VLC systems, the communication functionality is secondary to illumination. In particular, the modulating waveform is a bipolar signal superimposed over a DC bias that is set by the required illumination level. Therefore, the DC bias is excluded from SNR calculations, as suggested in [11].

Alice is equipped with N_{A} transmitters, i.e., there are N_{A} light fixtures utilized for illumination and data transmission. Each fixture consists of J LEDs. The electrical current fed into the light fixtures can be expressed by

$$\mathbf{I} = \mathbf{P}_{\mathrm{DC}} + \mathbf{x} \tag{1}$$

where $\mathbf{I} = [I_1\ I_2 \cdots I_{N_{\mathrm{A}}}]^{\mathrm{T}} \in \mathcal{R}_+^{N_{\mathrm{A}}}$, $\mathbf{P}_{\mathrm{DC}} = P_{\mathrm{DC}}\mathbf{1} \in \mathcal{R}_+^{N_{\mathrm{A}}}$ is the DC bias, and $\mathbf{x} \in \mathcal{R}^{N_{\mathrm{A}}}$ is the modulating signal vector. Notice that I_i, $i \in \{1, 2, \cdots N_{\mathrm{A}}\}$, is the current passing through every LED in the ith fixture, e.g., the LEDs in a single fixture are connected in series.

The transmitted signal $\mathbf{x}$ is subject to a per-fixture, i.e., per-antenna, peak constraint expressed by

$$|\mathbf{x}| \preceq \alpha \mathbf{P}_{\mathrm{DC}} \tag{2}$$

where $\alpha \in [0, 1]$ is the modulation index selected such that linearity is maintained over the LED operating range $P_{\mathrm{DC}} \pm \alpha P_{\mathrm{DC}}$.

We consider a deterministic Gaussian channel model. Bob and Eve are equipped with a single PD. Their received signals can be expressed by

$$y_{\mathrm{B}} = \mathbf{h}_{\mathrm{B}}^{\mathrm{T}}\mathbf{x} + z_{\mathrm{B}} \tag{3a}$$

$$y_{\mathrm{E}} = \mathbf{h}_{\mathrm{E}}^{\mathrm{T}}\mathbf{x} + z_{\mathrm{E}} \tag{3b}$$

where $y_{\{\cdot\}} \in \mathcal{R}$ is the PD output after removing the DC bias, $\mathbf{h}_{\{\cdot\}} \in \mathcal{R}_+^{N_{\mathrm{A}}}$ is the channel gain vector, and $z_{\{\cdot\}} \in \mathcal{R}$ is a zero-mean, additive white Gaussian noise (AWGN) sample with variance $\sigma_{\{\cdot\}}^2$. We assume that noise is also spatially white, i.e., $\sigma_{\mathrm{B}}^2 = \sigma_{\mathrm{E}}^2 = \sigma^2$.

For such Gaussian channel with amplitude constraint, it is appropriate to define the received SNR as the *peak* signal-to-noise ratio, i.e.,

$$\mathrm{SNR}_{\mathrm{B}} = \frac{\max\left\{\mathbf{h}_{\mathrm{B}}^{\mathrm{T}}\mathbf{x}\mathbf{x}^{\mathrm{T}}\mathbf{h}_{\mathrm{B}}\right\}}{\sigma^2} \tag{4a}$$

$$\mathrm{SNR}_{\mathrm{E}} = \frac{\max\left\{\mathbf{h}_{\mathrm{E}}^{\mathrm{T}}\mathbf{x}\mathbf{x}^{\mathrm{T}}\mathbf{h}_{\mathrm{E}}\right\}}{\sigma^2}. \tag{4b}$$

The channel gain $h_{ij} \in \mathcal{R}_+$ between the jth LED in the ith fixture and the PD at the receiver can be expressed by [12]

$$h_{ij} = \begin{cases} \frac{(m+1)A_{\mathrm{PD}}}{2\pi d_{ij}^2} \cos^m(\phi_{ij}) \frac{n^2}{\sin^2(\Psi_{\mathrm{C}})} \cos(\psi_{ij}) R & |\psi_{ij}| \leq \Psi_{\mathrm{C}} \\ 0 & |\psi_{ij}| > \Psi_{\mathrm{C}} \end{cases} \tag{5}$$

where $m = \frac{-\ln 2}{\ln(\cos \Phi_{\frac{1}{2}})}$ is the order of Lampertian emission with half illuminance at $\Phi_{\frac{1}{2}}$ (semi-angle), A_{PD} is the PD physical area, d_{ij} is the distance between the LED and PD, $\phi_{ij} < \frac{\pi}{2}$ is the angle of irradiance with respect to the axis normal to the transmitter surface, n is the refractive index of the optical concentrator located in front of the PD, $\Psi_{\mathrm{C}} \leq \frac{\pi}{2}$ is the receiver field of view (semi-angle at half received power), ψ_{ij} is the angle of incidence with respect to the axis normal to the receiver surface, and R is the PD responsivity.

The entries $h_i, i \in \{1, 2, \cdots N_{\mathrm{A}}\}$, of the channel gain vectors in (3) are obtained by the summation over J LEDs per fixture, i.e.,

$$h_i = \sum_{j=1}^{J} h_{ij}, \quad i \in \{1, 2, \cdots N_{\mathrm{A}}\}. \tag{6}$$

III. Secrecy Rates of VLC Channels

A. Secrecy Capacity of the Scalar VLC Channel

If Alice is equipped with a single light fixture, or if all the fixtures shall be modulated by the same electrical signal, e.g., due to hardware limitations, the resulting communication channel is SISO. The modulating signal x can be expressed by

$$\mathbf{x} = \alpha P_{\mathrm{DC}} \mathbf{1} d \tag{7}$$

where the data symbol d is normalized such that $d \in [-1, 1]$, without loss of generality. Therefore, (3) and (4) can be simplified to

$$y_{\mathrm{B}} = \alpha P_{\mathrm{DC}} \|\mathbf{h}_{\mathrm{B}}\|_1 d + z_{\mathrm{B}} \tag{8a}$$

$$y_{\mathrm{E}} = \alpha P_{\mathrm{DC}} \|\mathbf{h}_{\mathrm{E}}\|_1 d + z_{\mathrm{E}} \tag{8b}$$

$$\mathrm{SNR_B} = \frac{\alpha^2 P_{\mathrm{DC}}^2 \|\mathbf{h}_{\mathrm{B}}\|_1^2}{\sigma^2} \tag{9a}$$

$$\mathrm{SNR_E} = \frac{\alpha^2 P_{\mathrm{DC}}^2 \|\mathbf{h}_{\mathrm{E}}\|_1^2}{\sigma^2}. \tag{9b}$$

Such SISO wiretap channel is stochastically degraded when $\mathrm{SNR_B} \geq \mathrm{SNR_E}$, and therefore its secrecy capacity C_s is found by [13]

$$C_s = \left\{ \max_{p(d)} \mathbb{I}(d; y_{\mathrm{B}}) - \mathbb{I}(d; y_{\mathrm{E}}) \right\}^+, \quad \text{s.t.} \quad |d| \leq 1. \tag{10}$$

It is well-known that seeking a closed-form solution for the maximization problem in (10), with the peak constraint, is unfeasible [13], [14]. However, it was shown that the secrecy capacity-achieving distribution $p^*(d)$ exists and is unique. Furthermore, it is discrete with a finite number of mass points and can be efficiently found via numerical optimization techniques [13].

A properly-designed illumination system should exhibit small spatial variations in light intensity across the illuminated area. Consequently, for a SISO VLC scenario, achievable secrecy rates would be practically negligible, if not equal to zero.

B. The MISO Channel – Null-Steering

When Alice is equipped with multiple light fixtures and perfectly knows Eve's CSI, she can utilize beamforming to significantly increase achievable secrecy rates to Bob. A suboptimal, but essentially simple, strategy is to zero-force Eve's reception. A closed-form null direction $\mathbf{w} \in \mathcal{R}^{N_{\mathrm{A}}}$ can be obtained by projecting Bob's channel onto the nullspace of Eve [5], i.e.,

$$\mathbf{w} = k \mathbf{\Psi}_{\mathrm{E}} \mathbf{\Psi}_{\mathrm{E}}^{\mathrm{T}} \mathbf{h}_{\mathrm{B}} \tag{11}$$

where $\mathbf{\Psi}_{\mathrm{E}} \in \mathcal{R}^{N_{\mathrm{A}} \times N_{\mathrm{A}}-1}$ is a matrix whose $N_{\mathrm{A}} - 1$ columns constitute a basis for the nullspace of $\mathbf{h}_{\mathrm{E}}^{\mathrm{T}}$ and k is a constant such that $|\mathbf{w}| \preceq \mathbf{1}$.

Therefore, the transmitted signal can be expressed by

$$\mathbf{x} = \alpha P_{\mathrm{DC}} \mathbf{w} d \tag{12}$$

where d is the data symbol as defined for (7). Then, (3) and (4) specialize to

$$y_{\mathrm{B}} = \alpha P_{\mathrm{DC}} \mathbf{h}_{\mathrm{B}}^{\mathrm{T}} \mathbf{w} d + z_{\mathrm{B}} \tag{13a}$$

$$y_{\mathrm{E}} = z_{\mathrm{E}} \tag{13b}$$

$$\mathrm{SNR_B} = \frac{\alpha^2 P_{\mathrm{DC}}^2 \mathbf{h}_{\mathrm{B}}^{\mathrm{T}} \mathbf{w} \mathbf{w}^{\mathrm{T}} \mathbf{h}_{\mathrm{B}}}{\sigma^2} \tag{14a}$$

$$\mathrm{SNR_E} = 0. \tag{14b}$$

When Eve's reception is forced to zero, any achievable rate between Alice and Bob is secure. Consequently, the achievable secrecy rate is upper bounded by the capacity of the equivalent single-stream Alice-Bob channel, i.e.,

$$R_s = \max_{p(d)} \mathbb{I}(d; y_{\mathrm{B}}), \quad \text{s.t.} \quad |d| \leq 1. \tag{15}$$

Similar to (10), the maximization problem in (15) shall be solved numerically to find the optimal discrete distribution $p^*(d)$ with finite number of mass points [14].

Notice that, unlike the Gaussian MISO wiretap channel considered in [5], it was not proved that beamforming is optimal for the Gaussian MISO wiretap channel subject to amplitude constraints. In addition, zero-forcing is not necessarily the optimal beamforming strategy, in particular at asymptotically low $\mathrm{SNR_B}$. Furthermore, the zero-forcing beamformer in (11) is suboptimal as it does not necessarily maximize $\mathrm{SNR_B}$. We leave more careful selection of the beamforming direction to future work.

C. The MISO Channel – Artificial Noise Transmission

The assumption that Eve's CSI is perfectly known to Alice is justifiable only in some scenarios, e.g., Eve is an authorized user in the network but confidential messages shall be exchanged between Alice and Bob. On the other hand, if Eve is a passive eavesdropper or a malicious user not registered in the network, such assumption is not valid.

A simple approach to secure the transmission to Bob without Eve's CSI is to attempt jamming Eve's reception. Alice could transmit randomly-generated noise symbols in the nullspace of Bob with the hope that considerable interference will be added at Eve's receiver [7], [8]. In a VLC scenario, Alice's optical power is divided into two distinctive groups of signals, the information-bearing signal steered towards Bob's channel, and jamming signals transmitted in Bob's nullspace.

Let $\hat{\mathbf{h}}_{\mathrm{B}} = \frac{\mathbf{h}_{\mathrm{B}}}{\|\mathbf{h}_{\mathrm{B}}\|_1}$ be Bob's channel vector normalized such that $\left\|\hat{\mathbf{h}}_{\mathrm{B}}\right\|_1 = 1$. Also, let $\hat{\mathbf{\Psi}}_{\mathrm{B}} \in \mathcal{R}^{N_{\mathrm{A}} \times N_{\mathrm{A}}-1}$ be a matrix whose columns $\hat{\psi}_{\mathrm{B}_1}, \hat{\psi}_{\mathrm{B}_2}, \cdots \hat{\psi}_{\mathrm{B}_{N_{\mathrm{A}}-1}}$ constitute a basis for the nullspace of $\mathbf{h}_{\mathrm{B}}^{\mathrm{T}}$ and are normalized such that $\left\|\hat{\psi}_{\mathrm{B}_i}\right\|_1 = 1, \forall i \in \{1, 2, \cdots N_{\mathrm{A}} - 1\}$. Let $\rho \in [0, 1]$ be the optical power, or equivalently the electrical signal amplitude, fraction devoted to data symbols, while $1-\rho$ is used for jamming symbols transmission. With the lack of Eve's CSI, it is appropriate to equally divide the $1 - \rho$ optical power fraction among the available $N_{\mathrm{A}} - 1$ nullspace directions. Therefore, the transmitted signal can be expressed by

$$\mathbf{x} = k\alpha P_{\mathrm{DC}} \left(\rho \hat{\mathbf{h}}_{\mathrm{B}} d + \frac{1-\rho}{N_{\mathrm{A}} - 1} \sum_{i=1}^{N_{\mathrm{A}}-1} \hat{\psi}_{\mathrm{B}_i} j_i \right) \tag{16}$$

where $d \in [-1, 1]$ is the data symbol, $j_i \in [-1, 1], i \in \{1, 2, \cdots N_{\mathrm{A}} - 1\}$, are jamming symbols, and k is a constant such that the peak constraint

$$k \left(\rho \left| \hat{\mathbf{h}}_{\mathrm{B}} \right| + \frac{1-\rho}{N_{\mathrm{A}} - 1} \sum_{i=1}^{N_{\mathrm{A}}-1} \left| \hat{\psi}_{\mathrm{B}_i} \right| \right) \preceq \mathbf{1} \tag{17}$$

is satisfied. Therefore, (3) and (4) specialize to

$$y_{\mathrm{B}} = k\alpha P_{\mathrm{DC}} \rho \mathbf{h}_{\mathrm{B}}^{\mathrm{T}} \hat{\mathbf{h}}_{\mathrm{B}} d + z_{\mathrm{B}} \tag{18a}$$

$$y_{\mathrm{E}} = k\alpha P_{\mathrm{DC}} \mathbf{h}_{\mathrm{E}}^{\mathrm{T}} \left(\rho \hat{\mathbf{h}}_{\mathrm{B}} d + \frac{1-\rho}{N_{\mathrm{A}} - 1} \sum_{i=1}^{N_{\mathrm{A}}-1} \hat{\psi}_{\mathrm{B}_i} j_i \right) + z_{\mathrm{E}} \tag{18b}$$

$$\mathrm{SNR}_{\mathrm{B}} = \frac{k^2 \rho^2 \alpha^2 P_{\mathrm{DC}}^2 \mathbf{h}_{\mathrm{B}}^{\mathrm{T}} \hat{\mathbf{h}}_{\mathrm{B}} \hat{\mathbf{h}}_{\mathrm{B}}^{\mathrm{T}} \mathbf{h}_{\mathrm{B}}}{\sigma^2} \tag{19a}$$

$$\mathrm{SINR}_{\mathrm{E}} = \frac{k^2 \rho^2 \alpha^2 P_{\mathrm{DC}}^2 \mathbf{h}_{\mathrm{E}}^{\mathrm{T}} \hat{\mathbf{h}}_{\mathrm{B}} \hat{\mathbf{h}}_{\mathrm{B}}^{\mathrm{T}} \mathbf{h}_{\mathrm{E}}}{k^2 \left(\frac{1-\rho}{N_{\mathrm{A}}-1} \right)^2 \alpha^2 P_{\mathrm{DC}}^2 \sum_{i=1}^{N_{\mathrm{A}}-1} \mathbf{h}_{\mathrm{E}}^{\mathrm{T}} \hat{\psi}_{\mathrm{B}_i} \hat{\psi}_{\mathrm{B}_i}^{\mathrm{T}} \mathbf{h}_{\mathrm{E}} + \sigma^2}. \tag{19b}$$

Notice that (19b) involves an approximation in the sense that the interference power term in the denominator is obtained using the peak power of the interference symbols $j_i \in [-1, 1], i \in \{1, 2, \cdots N_{\mathrm{A}} - 1\}$, which is one. Then, for a given ρ, the secrecy rate is found by numerically solving

$$R_s = \left\{ \max_{p(d)} \mathbb{I}(d; y_{\mathrm{B}}) - \mathbb{I}(d; y_{\mathrm{E}}) \right\}^+, \quad \text{s.t.} \quad |d| \leq 1. \tag{20}$$

Several performance measures can be considered for the optimal selection of ρ. In [8], a quality-of-service (QoS) constraint, expressed by a minimum threshold for $\mathrm{SNR}_{\mathrm{B}}$, was considered. For indoor VLC, we propose maximizing the average secrecy rate $\mathbb{E}\{R_s\}$ obtained by averaging over all possible locations for Eve. For a VLC network within a room of area A_{rm}, ρ is selected to maximize

$$\mathbb{E}\{R_s\} = \frac{1}{A_{\mathrm{rm}}} \iint R_s(x, y)\, dxdy \tag{21}$$

where x and y are the coordinates along the room width and length directions, respectively.

TABLE I. SIMULATION PARAMETERS [12], [15].

Problem geometry	
Room size $(W \times L \times H)$	$5 \times 5 \times 3$ m^3
Fixtures (Alice) height above floor level	2.5 m
Receivers (Bob and Eve) height above floor level	0.85 m
Number of light fixtures N_{A}	$4 = 2 \times 2$
Fixture pitch (center to center)	2.5 m
Number of LEDs per fixture J	$3600 = 60 \times 60$
LED pitch (within a fixture)	1 cm
Transmitter characteristics	
Average optical transmit power per LED P_{DC}	20 mW
LED half-angle at half luminous intensity $\Phi_{\frac{1}{2}}$	70°
Modulation index α	10%
Receiver characteristics	
PD geometrical area A_{PD}	1 cm^2
PD field of view (half-angle) Ψ_{C}	60°
PD responsivity R	0.54 (mA/mW)
Lens refractive index n	1.5
Noise power (averaged over the room area) σ^2	1.47×10^{-13}A^2

Notice that although the transmission strategy in (16) does not exploit Eve's CSI, such information is still required to select the secure transmission rate (20) [5].

IV. Simulation Results and Discussions

We obtained our simulation results using the parameters provided in [12], [15] and summarized in Table I. The room dimensions are $5 \times 5 \times 3$ m^3. Alice is equipped with four light fixtures located around the room center at height 2.5 m above the floor level. Each fixture consists of 60×60 LEDs and the average optical power per LED, set by the applied DC bias, is 20 mW. Bob and Eve are located at height 0.85 m above the floor level, e.g., on desks, and their receivers are equipped with a single PD. The modulation index is set to 10%. Noise is temporarily and spatially white with variance 1.47×10^{-13}A^2. Optimal probability distributions $p^*(d)$ were found via numerical optimization using MATLAB optimization toolbox [16].

A. The SISO Case

Figure 2 shows the spatial distribution of $\mathrm{SNR}_{\mathrm{E}}$ (9b) within the room area when all the light fixtures are modulated by the same signal. As can be seen, $\mathrm{SNR}_{\mathrm{E}}$ ranges between 37.30 dB at the room corners and 50.93 dB directly underneath any of the four fixtures with an average of 47.18 dB. Notice that $\mathrm{SNR}_{\mathrm{E}}$ is higher than 43 dB in 91% of the room area. Such scenario is not promising from a security perspective since the probability that $\mathrm{SNR}_{\mathrm{E}} \leq \mathrm{SNR}_{\mathrm{B}}$ is low making secure communication on a physical-layer basis not practical for the SISO case. Figure 3 shows the secrecy capacity (10) as a function of Eve's location. C_s is zero in 34%

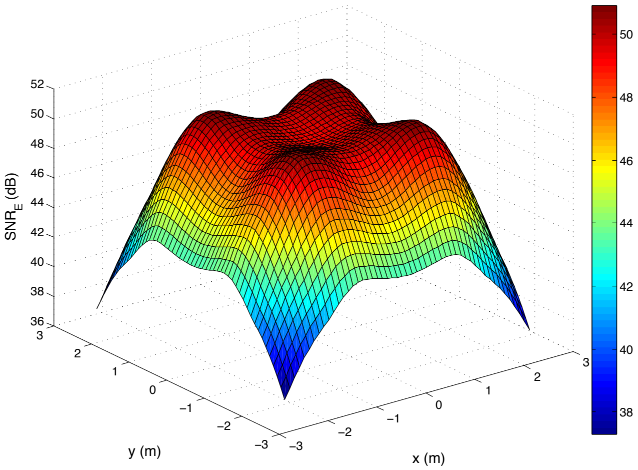

Fig. 2. SNR$_\mathrm{E}$ (9b) as a function of Eve's location for the SISO case.

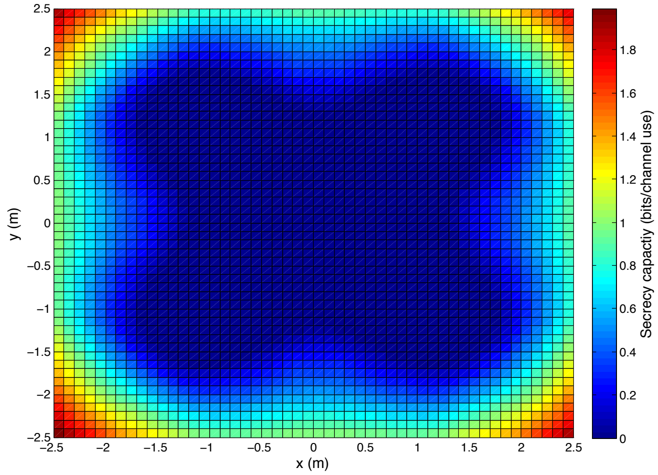

Fig. 3. Secrecy capacity (10) as a function of Eve's location for the SISO case. (Bob is located at the room center.)

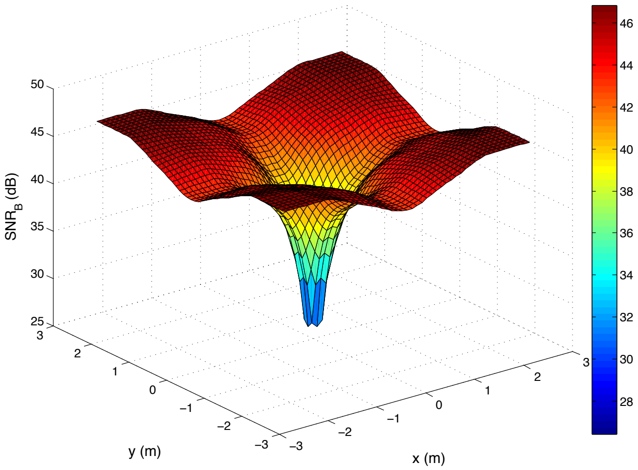

Fig. 4. SNR$_\mathrm{B}$ (14a) as a function of Eve's location for the MISO case with null-steering. (Bob is located at the room center.)

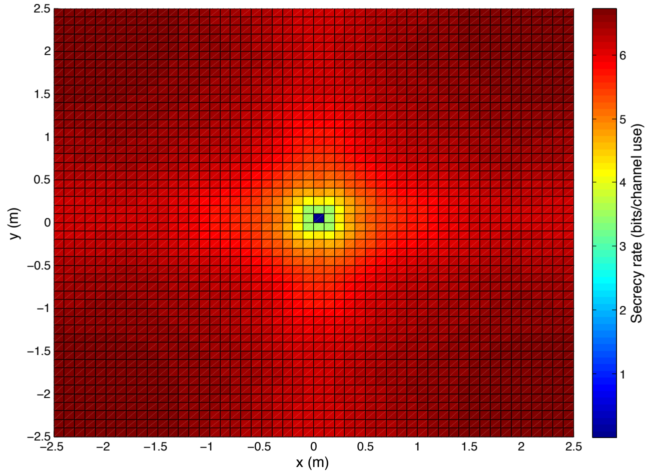

Fig. 5. Secrecy rate (15) as a function of Eve's location for the MISO case with null-steering. (Bob is located at the room center.)

of the room area, less than 1 bit/channel use in 90% of the room area, and reaches its maximum of 1.99 bits/channel use when Eve is located at any of the room corners. Secrecy capacity averaged over the room area at height 0.85 m is 0.40 bits/channel use.

B. The MISO Case with Null-Steering

Figure 4 shows SNR$_\mathrm{B}$ (14a) as a function of Eve's location when the zero-forcing beamformer (11) is applied. The achievable secrecy rate (15) is shown in Fig. 5. It can be seen that R_s is positive unless Bob and Eve are in the same location. The average secrecy rate is 6.31 bits/channel use with a maximum of 6.73 bits/channel use when Eve is located at any of the room corners. It is obvious that utilizing Eve's CSI via null-steering significantly increases the achievable secrecy rate compared to the SISO case.

C. The MISO Case with Artificial Noise Transmission

Figure 6 shows SINR$_\mathrm{E}$ (19b) as a function of Eve's location when artificial noise transmission (16) is employed with $\rho = 0.5$. The achievable secrecy rate (20) is shown in Fig. 7. It can be seen that R_s is positive unless Eve is located at the room center. The average secrecy rate is 5.32 bits/channel use, i.e., about 1 bit/channel use less than the null-steering case.

The effect of ρ on the average secrecy rate (21) is shown in Fig. 8. As can be seen, the optimum value for ρ that maximizes the average secrecy rate is located around 0.5. Such value depends on Bob's location. Also, the average secrecy rate is, in general, better than the SISO secrecy capacity (10) even with $\rho = 1$ since SNR$_\mathrm{E}$ is reduced via beamforming towards Bob's channel.

V. Conclusions

In this paper, we proposed improving the confidentiality of VLC links via physical-layer security techniques. To the best of our knowledge, such approach has not been considered before. We numerically evaluated achievable secrecy rates for three typical VLC scenarios. For the SISO case, achievable secrecy

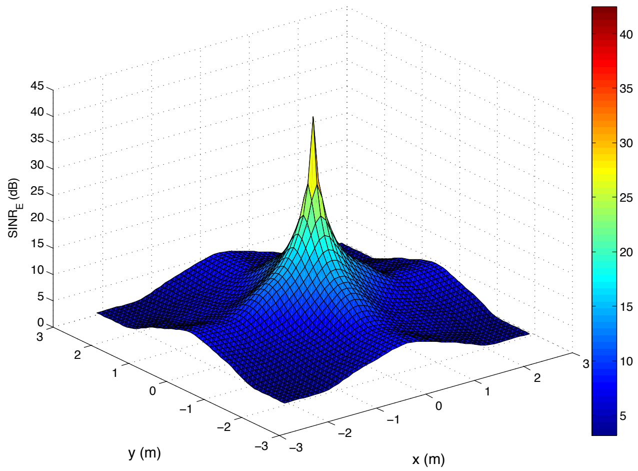

Fig. 6. SINR$_\mathrm{E}$ (19b) as a function of Eve's location for the MISO case with artificial noise transmission ($\rho = 0.5$). (Bob is located at the room center.)

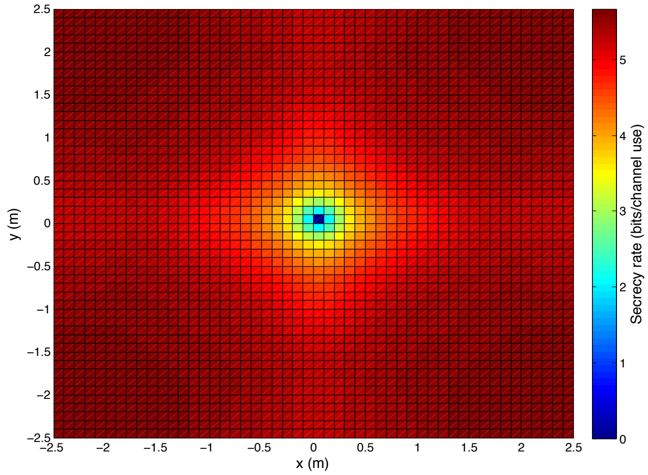

Fig. 7. Secrecy rate (20) as a function of Eve's location for the MISO case with artificial noise transmission ($\rho = 0.5$). (Bob is located at the room center.)

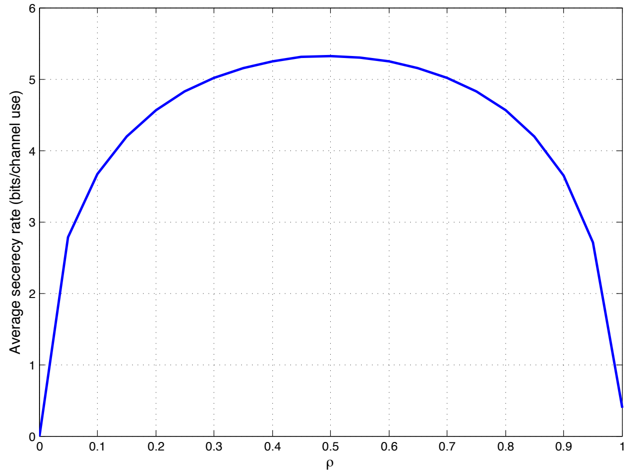

Fig. 8. Average secrecy rate (21) as a function of ρ for the MISO case with artificial noise transmission. (Bob is located at the room center.)

rates are negligible. When beamforming is applicable at the transmitter, secrecy rates can be significantly improved via null-steering if the eavesdropper's CSI is available. With the lack of the eavesdropper's CSI, secure transmission is still possible via artificial noise transmission in the receiver's nullspace.

In our ongoing research, we shall investigate robust beamforming strategies when the transmitter has imperfect receiver's and/or eavesdropper's CSI. In addition, multi-user and multiple-eavesdropper scenarios are interesting subjects for further research.

References

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

[2] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, pp. 1355–1387, 1975.

[3] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[4] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[5] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 3088–3104, 2010.

[6] ——, "Secure transmission with multiple antennas—part II: The MIMOME wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5515–5532, 2010.

[7] R. Negi and S. Goel, "Secret communication using artificial noise," in *2005 IEEE 62nd Vehicular Technology Conference, 2005. VTC-2005-Fall.*, vol. 3, 2005, pp. 1906–1910.

[8] A. Swindlehurst, "Fixed SINR solutions for the MIMO wiretap channel," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, April 2009, pp. 2437–2440.

[9] A. Puryear and V. W. S. Chan, "Using spatial diversity to improve the confidentiality of atmospheric free space optical communication," in *2011 IEEE Global Telecommunications Conference (GLOBECOM 2011)*, Dec 2011, pp. 1–6.

[10] M. Agaskar and V. W. S. Chan, "Nulling strategies for preventing interference and interception of free space optical communication," in *2013 IEEE International Conference on Communications (ICC)*, June 2013, pp. 3927–3932.

[11] S. Dimitrov, S. Sinanovic, and H. Haas, "Signal shaping and modulation for optical wireless communication," *Journal of Lightwave Technology*, vol. 30, no. 9, pp. 1319–1328, 2012.

[12] T. Komine and M. Nakagawa, "Fundamental analysis for visible-light communication system using LED lights," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 1, pp. 100–107, 2004.

[13] O. Ozel, E. Ekrem, and S. Ulukus, "Gaussian wiretap channel with an amplitude constraint," in *2012 IEEE Information Theory Workshop (ITW)*, Sept 2012, pp. 139–143.

[14] J. G. Smith, "The information capacity of amplitude- and variance-constrained scalar Gaussian channels," *Journal of Information and Control*, vol. 18, pp. 203–219, 1971.

[15] L. Zeng, D. O'Brien, H. Minh, G. Faulkner, K. Lee, D. Jung, Y. Oh, and E. T. Won, "High data rate multiple input multiple output (MIMO) optical wireless communications using white LED lighting," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 9, pp. 1654–1662, 2009.

[16] MATLAB, *R2012b (8.0.0.783)*. Natick, Massachusetts: The MathWorks Inc., 2012.