

Physical Layer Security in Visible Light Communication Systems with Randomly Located Colluding Eavesdroppers

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

Abstract—This letter investigates the secrecy performance in visible light communication (VLC) in the presence of randomly located *colluding eavesdroppers* (EDs). Colluding EDs can combine their observations and degrade the secrecy performance of the VLC systems. Utilizing the numerical inversion of a characteristic function, the probability distribution of the combined signal-to-noise ratio of colluding EDs is analyzed. The closed-form expression of the secrecy outage probability is derived and verified by Monte Carlo simulations.

Index Terms—Physical layer security, visible light communication, stochastic geometry, secrecy outage probability.

I. INTRODUCTION

Visible Light Communication (VLC) systems have gained great popularity among researchers and engineers as a possible solution for offloading the high traffic from the capacity-stressed macrocells in future networks. VLC is an enabling technology that uses visible light as its communication medium and exploits the light infrastructure currently being used for illumination to provide high-speed indoor wireless communication [1].

Since visible light cannot penetrate an opaque wall, a VLC system can offer high security at the physical layer. However, in large rooms, such as offices, libraries, and shopping malls, there is always the possibility that an eavesdropper (ED) can wiretap the signal in the air. As one of many network security techniques, physical layer security (PLS) is a set of techniques that enable a transmitter and a legitimate receiver (UE) to securely transmit and receive important data utilizing the randomness of a channel to hide information from EDs at the cost of reducing communication rates [2].

To secure VLC systems, many PLS techniques for VLC systems have been studied [3]–[6]. All of these works assumed a single ED or non-colluding multiple EDs. However, spatially distributed multiple EDs in a VLC system can combine their observations by various diversity combining methods and significantly improve their combined signal-to-noise ratio (SNR), which can degrade the secrecy performance of the network. Moreover, in VLC systems, the collusion among multiple EDs would be a very feasible and practical way to improve the received SNR of EDs escaping the vigilance of the UE, because the EDs can easily maintain the appearance of ordinary legitimate receivers.

There have been a few studies regarding colluding EDs in radio frequency (RF) systems [7]–[9]. In [7], Win et al.

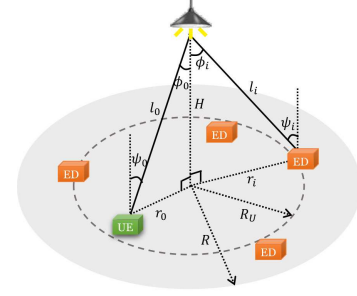


Fig. 1. A circular area configuration for VLC systems. An LED transmitter is attached to the center of the ceiling.

derived the stochastic expressions of the secrecy capacity in the presence of colluding EDs, and, in [8], analyzed how ED collusion degrades the secrecy properties of the UE, in comparison to a non-colluding scenario. In [9], Chen et al. proposed a transmit antenna selection and full-duplex jamming scheme to enhance secrecy performance when colluding EDs are present.

Motivated by these RF works, in this letter, we study the secrecy performance of a VLC system with randomly located colluding EDs. To the best of our knowledge, this work is the first to model and analyze the secrecy performance of VLC systems with colluding EDs. As in [5], to deal with the randomness of the VLC receivers, we apply a binomial point process (BPP) to model the UE location and a Poisson point process (PPP) to model the ED locations, respectively. However, contrary to [5], where the contact distribution of a PPP is simply used to analyze the probability density of the maximum SNR of non-colluding EDs, in this letter, the Gil-Pelaez numerical inversion formula [10] is used to analyze the combined SNR of EDs. The main contributions of this work are as follows:

- We characterize the probability density function (PDF) of the SNR of the UE and calculate the cumulative distribution function (CDF) of the combined SNR of the colluding EDs by numerically evaluating the Gil-Pelaez inversion formula of a characteristic function (CF).
- We derive the closed-form expression of the secrecy outage probability (SOP) in the presence of colluding EDs that adopt the maximum ratio combining (MRC) technique.

II. SYSTEM MODEL

In this letter, we consider the downlink of a VLC system as shown in Fig. 1. Multiple colluding passive EDs are assumed to be randomly distributed according to a homogeneous PPP with density λ_E in a circular area \mathcal{S} with radius R . Since it may be infeasible to know the number and locations of EDs in real VLC systems, modeling the EDs using tools from stochastic

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 was with the Department of Engineering Science, University of Oxford, and is now 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.

geometry would provide a more practical guideline to network designers for anticipating a secure transmission with a certain density of EDs. Also, one active UE is assumed to be randomly located according to a BPP in a circular area \mathcal{U} with radius R_U ($R_U < R$) to investigate the secrecy performance at the system level. An LED transmitter is located at the center of the ceiling, and H denotes the height of the ceiling from the work plane. All of the receivers are assumed to be located in the circular work plane.

A direct-current (DC) biased pulse-amplitude modulation (PAM) VLC scheme is considered [3], [5]. The data signal $s(t) \in \mathbb{R}$ in time slot t is superimposed on a fixed bias current $I_{DC} \in \mathbb{R}_+$. The fixed bias I_{DC} is used for the purpose of illumination. Thus, the transmitter's modulated signal $x(t)$ of $s(t)$ is a zero-mean current signal that can be expressed by $x(t) = \alpha I_{DC} s(t)$, where $\alpha \in [0, 1]$ is termed the modulation index. To maintain linear current-to-light conversion, the amplitude of $x(t)$ is constrained such that $|x(t)| \leq \alpha I_{DC}$. Thus, the dynamic range of the LED is $I_{DC} \pm \alpha I_{DC}$. Also, since $\mathbb{E}[x(t)] = 0$, the modulated signal does not affect illumination.

Therefore, the VLC channel model at the i th receiver can be written as

$$y_i(t) = h_i x(t) + n_i(t) \quad (1)$$

where h_i is the channel transfer coefficient from the transmitter to the i th receiver. We allocate $i = 0$ to the UE and $i > 0$ to the EDs. $n_i(t)$ is the zero-mean additive white Gaussian noise (AWGN) at the i th receiver. As a result of collusion, EDs are assumed to use the MRC technique, which maximizes the combined SNR in VLC systems [11]. Thus, the combined signal of EDs can be written as

$$y_{\Phi_E}(t) = \sum_{i \in \Phi_E} h_i y_i = \rho_{\Phi_E}^2 x(t) + n_{\Phi_E}(t) \quad (2)$$

where $\rho_{\Phi_E}^2 = \sum_{i \in \Phi_E} h_i^2$ and $n_{\Phi_E}(t) = \sum_{i \in \Phi_E} h_i n_i(t)$.

According to [12], the channel gain $h_i \in \mathbb{R}_+$ in a VLC system corresponding to an LED with a generalized Lambertian emission pattern is given by

$$h_i = \begin{cases} \eta \frac{(m+1)A_{PD}}{2\pi l_i^2} \frac{\kappa^2 \cos^m(\phi_i)}{\sin^2(\Psi_c)} \cos(\psi_i) RT & \text{for } |\psi_i| \leq \Psi_c, \\ 0 & \text{for } |\psi_i| > \Psi_c \end{cases} \quad (3)$$

where η (W/A) 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 angle $\phi_{1/2}$, and A_{PD} is the physical area of the photodiode (PD). As shown in Fig. 1, l_i is the distance between the transmitter and the i th receiver, and r_i denotes the distance between the transmitter and the i th receiver in the work plane. ϕ_i is the angle of irradiance, and ψ_i is the angle of incidence. Also, κ is the refractive index of the optical concentrator at the receiver, Ψ_c denotes the received field of view of the PD, R is the photodetector's responsivity, and T (V/A) is the transimpedance amplifier gain. Moreover, by assuming that a receiver's PD faces up normal to the work plane, we can rewrite (3) in terms of l_i as

$$h_i = \eta \frac{(m+1)A_{PD}}{2\pi l_i^2} \frac{\kappa^2}{\sin^2(\Psi_c)} \left(\frac{Z}{l_i}\right)^m \left(\frac{Z}{l_i}\right) RT = K l_i^{-(m+3)} \quad (4)$$

where $K = (\eta(m+1)A_{PD}Z^{m+1}\kappa^2 RT) / (2\pi \sin^2(\Psi_c))$. Note that (4) is valid only when $|\psi_i| \leq \Psi_c$ is satisfied. Thus, for the sake of simplicity, we assume that all of the receivers are located such that $l_i \leq H/\cos(\Psi_c)$ is satisfied for all i . This assumption can be justified since the channel gain decays like $l_i^{-(m+3)}$ as the receiver moves away from the LED; thus the receivers far from the LED can be ignored.

For the Gaussian VLC channel with amplitude constraints, it is appropriate to define the received SNR as the peak SNR since the channel capacity bounds of VLC systems are expressed as a function of the peak SNR [3]. Thus, the peak SNR at the i th receiver can be written as

$$\gamma_i = \frac{\alpha^2 I_{DC}^2 h_i^2}{\sigma^2} = \xi g(l_i) \quad (5)$$

where $\xi = \alpha^2 I_{DC}^2 K^2 / \sigma^2$ and $g(l_i) = l_i^{-2(m+3)}$. We use SNR to denote the peak, rather than average, SNR for the remainder of the paper. Also, the combined SNR of EDs with MRC can be defined as

$$\gamma_{\Phi_E} = \frac{\rho_{\Phi_E}^4 I_{DC}^2 \alpha^2}{\rho_{\Phi_E}^2 \sigma^2} = \sum_{i \in \Phi_E} \frac{h_i^2 I_{DC}^2 \alpha^2}{\sigma^2} = \sum_{i \in \Phi_E} \xi g(l_i). \quad (6)$$

The secrecy rate of the VLC channel is given by [2]

$$C_s = \max_{p_X} (\mathbb{I}(X; Y_0) - \mathbb{I}(X; Y_{\Phi_E})), \quad (7a)$$

$$\text{s.t. } |x| \leq \alpha I_{DC} \quad (7b)$$

where p_X is the input distribution and $\mathbb{I}(\cdot; \cdot)$ denotes the mutual information. It is infeasible to calculate the closed-form solution for (7) due to the amplitude constraint [13]. Thus, in the following, we provide the closed-form of an achievable secrecy rate for colluding EDs.

Lemma 1. *An achievable secrecy rate of the Gaussian wiretap channel in (1) for colluding EDs under the assumption that MRC is used by the EDs can be obtained by lower-bounding the secrecy capacity in (7) to give*

$$R_s = \max \left\{ \frac{1}{2} \log \left(\frac{3\pi e + 6\gamma_0}{3\pi e + \pi e \gamma_{\Phi_E}} \right), 0 \right\} \quad (8)$$

where $\log(\cdot)$ denotes the natural logarithm.

Proof. See Appendix A. \square

In addition, the classical SOP definition is the probability that the instantaneous secrecy capacity falls below a target secrecy rate [7]. However, since the closed-form of the secrecy capacity with the input amplitude constraint is also not readily available, we adopt the modified SOP for the analysis that the achievable secrecy rate R_s is lower than a threshold secrecy rate R_{th} , i.e.,

$$P_{SO} = \mathbb{P}(R_s \leq R_{th}). \quad (9)$$

III. SECRECY ANALYSIS WITH COLLUDING EDs

In this section, firstly, the probability distributions of γ_0 and γ_{Φ_E} are calculated. Secondly, the closed-form analytical expression for the SOP is derived.

A. Probability Distributions of γ_0 and γ_{Φ_E}

For the UE uniformly and randomly located in a circular area \mathcal{U} with radius R_U , the PDF of r_0 is $f_{r_0}(r_0) = 2r_0/R_U^2$ for $0 \leq r_0 \leq R_U$. The PDF of l_0 can be calculated to be $f_{l_0}(l_0) = 2l_0/R_U^2$ for $H \leq l_0 \leq \sqrt{R_U^2 + H^2}$ using the PDF transformation of random variables. Furthermore, once again using the transformation method, the PDF of γ_0 , i.e., the SNR of the UE, can be obtained from (5) to be

$$f_{\gamma_0}(y) = \frac{(y/\xi)^{-\frac{1}{m+3}}}{R_U^2(m+3)y} \quad \text{for } y_1 \leq y \leq y_2 \quad (10)$$

where $y_1 = \xi(R_U^2 + H^2)^{-(m+3)}$ and $y_2 = \xi H^{-2(m+3)}$.

Lemma 2. Numerically evaluating the Gil-Pelaez inversion of a CF [10], the CDF of γ_{Φ_E} can be calculated as

$$F_{\gamma_{\Phi_E}}(x) \approx \frac{1}{2} - \sum_{k=0}^K \frac{\text{Im} \left\{ \varphi_{\gamma_{\Phi_E}}((k+0.5)\Delta) e^{-j(k+0.5)\Delta x} \right\}}{\pi(k+0.5)} \quad (11)$$

for $0 \leq x \leq \infty$, where $\varphi_{\gamma_{\Phi_E}}(\omega)$ is the CF of γ_{Φ_E} given in (13) at the top of the next page, K and Δ denote the inversion parameters defined in [10], and $\Gamma(x, y)$ denotes an upper incomplete gamma function.

Proof. The CF of γ_{Φ_E} can be calculated as

$$\begin{aligned} \varphi_{\gamma_{\Phi_E}}(\omega) &= \mathbb{E} [e^{j\omega\gamma_{\Phi_E}}] = \mathbb{E} \left[\prod_{i \in \Phi_E} e^{j\omega\xi(r_i^2 + H^2)^{-(m+3)}} \right] \\ &\stackrel{(a)}{=} \exp \left(- \int_0^R \int_0^{2\pi} \lambda_E r \left(1 - e^{j\omega\xi(r^2 + H^2)^{-(m+3)}} \right) dr d\theta \right) \end{aligned} \quad (12)$$

where the closed-form expression of (12) is given in (13) at the top of the next page. Here, (a) applies the probability generation functional lemma (PGFL) of the PPP [14]. Then, using the numerical inversion of the CF proposed in [10], the CDF of γ_{Φ_E} can be obtained as in (11). \square

B. Secrecy Outage Probability

According to (9), the SOP can be written as

$$\begin{aligned} P_{SO} &= \mathbb{P}(R_s \leq R_{th}) = \mathbb{P} \left(\frac{1}{2} \log \left(\frac{3\pi e + 6\gamma_0}{3\pi e + \pi e \gamma_{\Phi_E}} \right) \leq R_{th} \right) \\ &= \mathbb{P} \left(\gamma_0 \leq \nu \gamma_{\Phi_E} + 3\nu - \frac{\pi e}{2} \right) \end{aligned} \quad (14)$$

where $\nu = \pi e^{2R_{th}+1}/6$. Then, the closed-form of (14) can be calculated in (15) at the top of the next page, where $\mu = (-3\nu + \pi e/2)/\nu$ and $\varphi_{\gamma_{\Phi_E}}^*(\omega)$ denotes the conjugate of the CF. (a) holds due to $\text{Im}\{z\} = (z - z^*)/2j$ and (b) uses (2.325.6) in [15].

IV. NUMERICAL RESULT

In this section, theoretical and simulation results are given to validate our analysis. The simulation results are obtained by averaging over 10^5 independent Monte Carlo trials. We use $K = 8 \times 10^3$ and $\Delta = 2 \times 10^{-7}$ according to [10] for the numerical inversion. On a standard PC using MATLAB, the calculation can be executed in a couple of seconds.

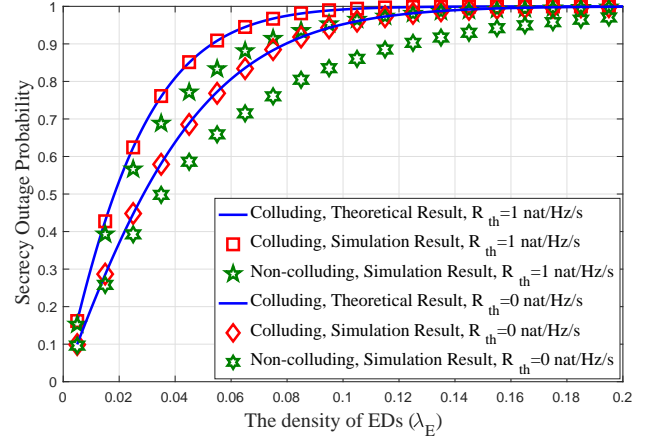


Fig. 2. Theoretical vs simulation secrecy outage probabilities for one BPP UE and multiple colluding EDs with different density λ_E , where $R = 6\text{m}$, $R_U = 2\text{m}$, $H = 3\text{m}$, $\psi_{1/2} = 60^\circ$, $\Psi_c = 70^\circ$, $A_{PD} = 1\text{cm}^2$, $\kappa = 1.5$, $T = 1V/A$ and $\sigma^2 = -128\text{dBm}$ are used.

Fig. 2 shows the simulation and theoretical results for the SOP with the configuration of one BPP UE and homogeneous bounded PPP EDs as the density of EDs λ_E increases. Firstly, it is obvious that the theoretical and numerical results match well, which validates our proposed analytical models. Furthermore, we note that the SOP increases as λ_E increases, since increasing λ_E brings more EDs, which enables them to achieve a higher SNR through collusion.

In addition, the simulation result for non-colluding PPP EDs is also given in the figure, which was investigated in [5]. In [5], the *maximum* SNR of multiple EDs was considered to determine the secrecy outage. While the SOP of colluding EDs is higher than that of non-colluding EDs for the entire range of λ_E , the SOP difference between colluding and non-colluding cases changes according to λ_E . More specifically, for the region of λ_E less than 0.01, the SOPs for the colluding and non-colluding cases are almost identical, since a single ED cannot collude alone. Note that when $\lambda_E = 0.01$, the average number of EDs given the room configuration is 1.13. When $\lambda_E = 0.055$, the SOP of colluding EDs with $R_{th} = 1\text{nat/Hz/s}$ is 0.076 higher than that of non-colluding EDs, but it decreases to 0.0082 when $\lambda_E = 0.155$. This difference comes from the fact that the colluding and non-colluding EDs exploit the different types of diversity combining techniques, i.e., MRC and selective combining [16], respectively, and each combining technique yields a different diversity gain according to the number of diversity branches, i.e., $\lambda_E \pi R^2$.

V. CONCLUSION

In this letter, the SOP was derived as a function of the density of EDs λ_E . To deal with randomly located UE and colluding EDs, we applied tools from stochastic geometry. This analysis was validated via theoretical and simulation results. Also, we verified that the collusion of EDs could degrade the secrecy performance of VLC systems, compared to the non-colluding scenario.

$$\varphi_{\gamma_{\Phi_E}}(\omega) = \exp \left(-\lambda_E \pi R^2 \left(1 + \frac{(-j\omega\xi)^{\frac{1}{m+3}}}{R^2(m+3)} \left(\Gamma \left(\frac{-1}{m+3}, -j\omega\xi H^{-2(m+3)} \right) - \Gamma \left(\frac{-1}{m+3}, -j\omega\xi (R^2 + H^2)^{-(m+3)} \right) \right) \right) \right) \quad (13)$$

$$\begin{aligned} P_{SO} &= \int_{y_1}^{y_2} \int_{\frac{y_2-3v+\pi e/2}{v}}^{\frac{y_2-3v+\pi e/2}{v}} f_{\gamma_{\Phi_E}}(x) f_{\gamma_0}(y) dx dy + \int_{y_1}^{y_2} \int_{\frac{y_2-3v+\pi e/2}{v}}^{\infty} f_{\gamma_{\Phi_E}}(x) f_{\gamma_0}(y) dx dy \\ &= \int_{y_1}^{y_2} \left(F_{\gamma_{\Phi_E}}(y_2/v + \mu) - F_{\gamma_{\Phi_E}}(y/v + \mu) \right) f_{\gamma_0}(y) dy + \int_{y_2/v+\mu}^{\infty} f_{\gamma_{\Phi_E}}(x) dx \int_{y_1}^{y_2} f_{\gamma_0}(y) dy \\ &= F_{\gamma_{\Phi_E}}(y_2/v + \mu) - \int_{y_1}^{y_2} F_{\gamma_{\Phi_E}}(y/v + \mu) f_{\gamma_0}(y) dy + F_{\gamma_{\Phi_E}}(\infty) - F_{\gamma_{\Phi_E}}(y_2/v + \mu) \\ &\stackrel{(a)}{\approx} 1 - \int_{y_1}^{y_2} \left(\frac{1}{2} + j \sum_{k=0}^K \frac{\varphi_{\gamma_{\Phi_E}}((k+0.5)\Delta) e^{-j(k+0.5)\Delta(y/v+\mu)} - \varphi_{\gamma_{\Phi_E}}^*((k+0.5)\Delta) e^{j(k+0.5)\Delta(y/v+\mu)}}{2\pi(k+0.5)} \right) \frac{(y/\xi)^{-\frac{1}{m+3}}}{R U^2(m+3)y} dy \\ &\stackrel{(b)}{=} 1 - \left(\frac{\left(y_2^{\frac{1}{m+3}} - y_1^{\frac{1}{m+3}} \right) (y_1 y_2 / \xi)^{\frac{-1}{m+3}}}{2 R U^2} + j \sum_{k=0}^K \left(\frac{2^{\frac{-1}{m+3}} e^{-j \frac{(1+2k)\Delta\mu}{2}} (y/\xi)^{\frac{-1}{m+3}}}{R U^2 \pi (1+2k)(m+3)} \left(-e^{-j(1+2k)\Delta\mu} (-j(1+2k)\Delta)^{\frac{1}{m+3}} \varphi_{\gamma_{\Phi_E}}^*((k+0.5)\Delta) \right. \right. \right. \\ &\quad \cdot \left. \left. \left(\Gamma \left(\frac{-1}{m+3}, \frac{-j(1+2k)y_1\Delta}{2v} \right) - \Gamma \left(\frac{-1}{m+3}, \frac{-j(1+2k)y_2\Delta}{2v} \right) \right) + (j(1+2k)\Delta)^{\frac{1}{m+3}} \varphi_{\gamma_{\Phi_E}}((k+0.5)\Delta) \right. \right. \\ &\quad \cdot \left. \left. \left(\Gamma \left(\frac{-1}{m+3}, \frac{j(1+2k)y_1\Delta}{2v} \right) - \Gamma \left(\frac{-1}{m+3}, \frac{j(1+2k)y_2\Delta}{2v} \right) \right) \right) \right) \right) \end{aligned} \quad (15)$$

APPENDIX A PROOF OF THE LEMMA 1

A lower bound on the secrecy rate of (8) can be obtained as follows

$$\begin{aligned} C_s &= \max_{p_X} (\mathbb{I}(X; Y_0) - \mathbb{I}(X; Y_{\Phi_E})) \\ &= \max_{p_X} (\mathbb{h}(Y_0) - \mathbb{h}(Y_0|X) - \mathbb{h}(Y_{\Phi_E}) + \mathbb{h}(Y_{\Phi_E}|X)) \\ &= \max_{p_X} (\mathbb{h}(h_0 X + N_0) - \mathbb{h}(N_0) - \mathbb{h}(Y_{\Phi_E}) + \mathbb{h}(N_{\Phi_E})) \\ &\stackrel{(a)}{\geq} \max_{p_X} \left(\frac{1}{2} \log \left(e^{2\mathbb{h}(h_0 X)} + e^{2\mathbb{h}(N_0)} \right) - \frac{1}{2} \log 2\pi e \sigma^2 \right. \\ &\quad \left. - \frac{1}{2} \log 2\pi e \mathbb{V}\text{ar}\{Y_{\Phi_E}\} + \frac{1}{2} \log 2\pi e \rho_{\Phi_E}^2 \sigma^2 \right) \\ &\stackrel{(b)}{\geq} \frac{1}{2} \log \left(4\alpha^2 I_{DC}^2 h_0^2 + 2\pi e \sigma^2 \right) - \frac{1}{2} \log(2\pi e \sigma^2) \\ &\quad - \left(\frac{1}{2} \log 2\pi e \left(\frac{\rho_{\Phi_E}^4 \alpha^2 I_{DC}^2}{3} + \rho_{\Phi_E}^2 \sigma^2 \right) - \frac{1}{2} \log 2\pi e \rho_{\Phi_E}^2 \sigma^2 \right) \\ &= \frac{1}{2} \log \left(1 + \frac{2\alpha^2 I_{DC}^2 h_0^2}{\pi e \sigma^2} \right) - \frac{1}{2} \log \left(1 + \frac{\rho_{\Phi_E}^2 \alpha^2 I_{DC}^2}{3\sigma^2} \right) \\ &= \frac{1}{2} \log \left(\frac{3\pi e + 6\gamma_0}{3\pi e + \pi e \gamma_{\Phi_E}} \right) \end{aligned} \quad (16)$$

where $\mathbb{h}(\cdot)$ and $\mathbb{V}\text{ar}\{\cdot\}$ denote differential entropy and variance, respectively. (a) follows from lower-bounding $\mathbb{h}(h_0 X + N_0)$ using the entropy-power inequality and upper-bounding $\mathbb{h}(Y_{\Phi_E})$ using by the differential entropy of a Gaussian random variable with variance $\mathbb{V}\text{ar}\{Y_{\Phi_E}\}$. Then, (b) follows from dropping the maximization by choosing a uniform distribution on p_X over $[-\alpha I_{DC}, \alpha I_{DC}]$. Note that (16) is similar to [3, Theorem 1], except that γ_{Φ_E} is the sum of EDs' SNR. Also, since the upper bound of the SIMO channel is not readily available, in this letter, we only study the SOP corresponding to the achievable secrecy rate. Note that considering the lower bound of the secrecy capacity is the worst case from the secrecy perspective, which is more practical and important when engineering secure VLC

systems.

REFERENCES

- [1] H. Haas, L. Yin, Y. Wang, and C. Chen, "What is LiFi?" *J. Lightw. Technol.*, vol. 34, no. 6, pp. 1533–1544, Mar. 2016.
- [2] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.
- [3] 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.
- [4] M. A. Arfaoui, Z. Rezki, A. Ghrayeb, and M. S. Alouini, "On the secrecy capacity of MISO visible light communication channels," in *IEEE Globecom Washington D.C., USA*, Dec. 2016, pp. 1–7.
- [5] S. Cho, G. Chen, and J. P. Coon, "Secrecy analysis in visible light communication systems with randomly located eavesdroppers," in *2017 IEEE ICC Paris, France*, May 2017, pp. 475–480.
- [6] L. Yin and H. Haas, "Physical-layer security in multiuser visible light communication networks," *IEEE J. on Sel. Areas Commun.*, vol. 36, no. 1, pp. 162–174, Jan. 2018.
- [7] P. C. Pinto, J. Barros, and M. Z. Win, "Wireless physical-layer security: The case of colluding eavesdroppers," in *IEEE ISIT Seoul, South Korea*, Jun. 2009, pp. 2442–2446.
- [8] —, "Secure communication in stochastic wireless networks -Part II : maximum rate and collusion," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 139–147, Feb. 2012.
- [9] 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. Forensics Security*, vol. 12, no. 5, pp. 1195–1206, May 2017.
- [10] R. B. Davies, "Numerical inversion of a characteristic function," *Biometrika*, vol. 60, no. 2, pp. 415–417, 1973.
- [11] A. Tsiatmas, F. M. J. Willems, and S. Baggen, "Optimum diversity combining techniques for visible light communication systems," in *IEEE Globecom Austin, USA*, Dec. 2014, pp. 456–461.
- [12] 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.
- [13] O. Ozel, E. Ekrem, and S. Ulukus, "Gaussian wiretap channel with an amplitude constraint," in *IEEE ITW Lausanne, Switzerland*, Sep. 2012, pp. 5553–5563.
- [14] S. N. Chiu, D. Stoyan, W. S. Kendall, and J. Mecke, *Stochastic geometry and its applications; 3rd ed.*, ser. Wiley Series in Probability and Statistics. Hoboken, NJ: Wiley, 2013.
- [15] I. S. Gradshteyn and I. M. Ryzhik, *Table of integrals, series, and products*, 7th ed. Elsevier/Academic Press, 2007.
- [16] G. L. Stüber, *Principles of Mobile Communication*. Norwell, MA, USA: Kluwer Academic Publishers, 2001.